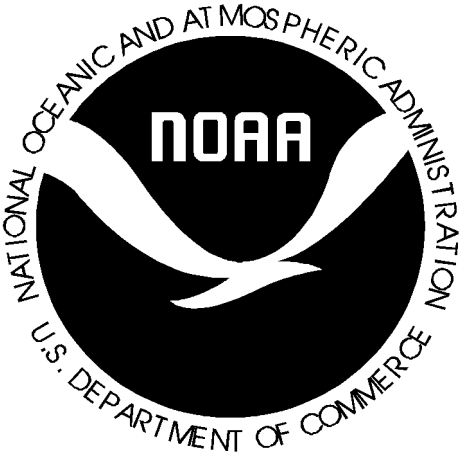
# NATIONAL OCEANIC AND ATMOSPHERIC ADMINISTRATION

# YEAR 2000 BUSINESS CONTINUITY AND CONTINGENCY PLAN




As of November 10, 1999

# Table of Contents

## 1.0 Background

The National Oceanic and Atmospheric(NOAA) and its predecessor organizations were pioneers in the use of computer technology. Over the approximately 40 years that computers have been in use, NOAA has developed customized software to handle both programmatic and administrative requirements. As is now well known, hardware and cost limitations often required the use of short-cut software techniques designed to conserve computing storage space. One such technique was to use two digits to reflect the 20th century. For dates beginning in the year 2000, this space saving technique will cause major errors and failures as programs will read "00" as 1900 instead of 2000.

NOAA's systems are, for the most part, not date centric(used for calculations, sorting, comparing, etc.). For example, the communications headers used to disseminate real-time weather data do not require any year or month element. The only date information contained in any disseminated weather product's data headers are the day of the month and Universal Time Coordinated(UTC) hour of the day. For example, in the 25th day of any month at 1700 hours UTC, the data header would read 251700. As for data processing purposes, only a very small subset of weather products contain any year information that is embedded in the data itself. Progress is well underway in modifying all software that processes this small subset of data. NOAA has created test Y2K data sets of these types of data and have made them available to many of the organizations that have external data exchanges with the NOAA. It also has been verified that there is no date issue with the satellite data.

Nonetheless, NOAA still must ensure that its computer systems, both hardware and software, will continue to function properly when they are called upon to process dates in 2000 and beyond. NOAA must ensure that legacy software is repaired, replaced, or retired; that commercial off-the-shelf software is compliant and will function properly; and that computer hardware is upgraded to process the correct date fields. NOAA is also ensuring that its physical systems at the various locations and on its platforms will be Y2K ready.

The solution to the problem cannot be postponed. Managing the successful completion of the necessary corrective actions is critical to NOAA operations and, more significantly, to the well-being of the Nation.

In recognition of the importance and the time-critical nature of the problem, in June 1996, NOAA established a Y2K Task Force chaired by the Manager for Systems Engineering of the Systems Acquisition Office with the participation by each of the Line and Staff Offices. The Task Force initially focused on promoting awareness of the Y2K problem; developing an inventory that determined problem magnitude; and preparing ROM cost estimates for implementing corrections. Subsequently, each Line and Staff Office developed a corrective action plan and became responsible for implementing it. The plans addressed the awareness, assessment, renovation, validation, and implementation phases as required in OMB directives. The Task Force reports regularly to the NOAA IT Board to ensure that NOAA's plans are on

track. In addition, the Deputy Under Secretary(DUS) meets quarterly and as necessary with the Offices to review progress on renovation, validation, and implementation efforts.

The awareness phase is a continuous process. As noted, the NOAA IT Board and DUS regularly review Y2K progress and issue and disseminate information updates throughout NOAA. The Y2K inventory, initially developed in June of 1996, was updated most recently in April 1998 and transmitted to the DOC for its Y2K database that will enable it to respond to inquiries more promptly and effectively.

NOAA's most recent OMB quarterly report for August 1999 reflected 117 mission-critical systems. This excludes the two AWIPS development systems(hardware and FSL software) that were removed from the reporting process and are monitored separately. Of the 117 systems, 116 systems are now compliant. NOS' Automated Distribution System-Client Server replacement system experienced procurement delays but is now undergoing extremely successful testing and will be implemented by September 30, 1999.

*Budget:* NOAA's estimated Y2K costs are $16,730K. The FY 1999 costs are estimated to be $10,737K. These are in addition to routine maintenance costs.

*Facilities:* Currently, the NOAA facilities Y2K database is carrying a total 540 DOC owned facilities and 268 leased facilities. These inventory numbers will change periodically due to closures, lease terminations, and related events. NOAA has DOC owned and leased facilities across the United States and locations on islands in the Pacific and Atlantic Oceans. To determine if there were any potential Year 2000 problems, in-house office personnel surveyed these components of NOAA. Letters were sent to the owners and landlords in the Washington metropolitan area and in the field for NOAA commercial leased facilities to ensure they are Y2K compliant. Various power and gas companies were contacted to inquire about their respective Y2K compliance programs. NOAA's Facilities Management Division has developed a formal Y2K Business Continuity and Contingency Plan for NOAA owned and commercial leased facilities within the Washington metropolitan area, field offices, and the Administrative Support Centers (ASCs).

NOAA is still conducting the Y2K compliance assessment of its owned and leased facilities. As of June 30, 1999, of the 540 DOC/ NOAA-owned facilities, 385 (71 percent) are Y2K compliant; 37 (7 percent) are not Y2K compliant; 8 (2 percent) assessments are still due; and 110 (20 percent) are/will be excess to GSA (i.e. NOAA will no longer be occupying the building). For the 268 DOC/NOAA leased facilities, 180 (67 percent) facilities are Y2K compliant; and 12 (4 percent) are not Y2K compliant; 50 (19 percent) assessments are still due; and 26 (10 percent) leases are/will be terminated (i.e. NOAA will no longer be occupying the building). The Y2K non-compliant facilities are primarily associated with the Heating Ventilation and Air-Conditioning controls which can be placed on manual operations.

NOAA provided a status of its Y2K compliance progress to the Department of Commerce's Real

Estate Group on April 2, 1999, for the continental United States (CONUS) and Non-CONUS facilities.

Compliance information from Potomac Electric Power Company (PEPCO) and the natural gas company in the Metropolitan Washington Area has been received. The NOAA owned and leased buildings are Y2K compliant. There was testing of one security system in Silver Spring Metro Center Building 3 which was found to be non- compliant. The software patch was installed in February for Y2K compliance.

*Motor Vehicles:* Information received from the NOAA motor pool manager stated that the NOAA vehicle fleet should not have any Y2K issues. None of the vehicle vendors nor GSA have contacted that office with any concerns.

*PC hardware and software*: For over two years, NOAA has been undertaking an aggressive PC upgrade following the FAR requirement of purchasing only PC hardware certified Y2K compliant. NOAA is using either the YMark 2000 free ware tool from the National Software Testing Laboratories or the Check2000 PC from Greenwich Mean Time to test for Year 2000 PC hardware compliance. No significant problems have been uncovered so far.

NOAA also has been following the FAR in the acquisition of COTS software. We are assessing the software Year 2000 compliance through information on vendor web sites, other agency web sites, e.g., GSA, and information technology literature.

*Scientific Equipment:* NOAA has completed an extensive inventory of all non-mission-critical scientific equipment which could have embedded chip Y2K issues. Vendors have been contacted and certificates of compliance are being obtained and follow-up testing is nearing completion, Equipment having Y2K compliance problems is being repaired/replaced.

*Avionics on NOAA Aircraft* - Rockwell International Corporation installed Y2K revisions to the avionics package on NOAA's Gulfstream G-IV jet during routine maintenance in May 1999. Independent Verification and Validation tests were overseen and approved by Government/non-vendor independent personnel. The avionics on the other, older NOAA aircraft are not date centric.

*Shipboard marine engine control, navigation, security, environmental, and monitoring systems:* The marine engine control and monitoring systems vendor upgrades/repairs were implemented and tested. Additionally, vendor publications, newsletters, and web sites are monitored for any Y2K issues. All ships under ONCO management will be in U.S. ports with their fuel tanks topped off on January 1, 2000. ONCO is in correspondence with field offices, ships, and aircraft to prepare a plan of activities for January 1, 2000. Activities will include a reporting scheme to advise all levels of management of any Y2K problems and solutions.

*Data Exchanges:* At the request of the DOC, NOAA completed the GAO survey of ingoing and

outgoing data exchanges. Three mission-critical systems(1 for the Office of Finance and Administration and 2 for the National Environmental Satellite, Data, and Information Service) which exchange data with outside organizations were identified with a total of 62 data exchanges. Of that number, 49 are with Federal Agencies, 7 with the private sector, and 6 with foreign governments. There are no system-to-system data exchanges that require transition plans or Memoranda of Understanding with State or local governments. A data exchange bridge has been developed for the OFA data exchanges with the Departments of Agriculture and Transportation. The DOC is the point of contact with the National Finance Center in Agriculture. The NESDIS data are non-date centric satellite data. NESDIS has made contact with all its partners and exchange formats have been finalized.

*Outreach/Awareness:* Through the NWS, NOAA continues to focus its Y2K outreach efforts primarily through the AMS and WMO. It also holds user conferences and maintains electronic bulletin boards to exchange information and issues. NOAA also continues to participate in information gathering by the White House on its Y2K outreach program. Information was collected on NOAA contacts with the following sectors: insurance; emergency preparedness; environmental protection; and science and technology. NOAA is represented on the cross-cutting Emergency Preparedness and Environmental Protection working groups being chaired by FEMA and EPA, respectively. The NWS also represents NOAA on the Catastrophic Disaster Recovery Group as part of the Federal Response Plan.

An NWS emergency-preparedness outreach plan addressing the private meteorology sector is complete. NWS and NESDIS are members of the NWS' Office of Federal Coordinator for Meteorology affiliated Special Action Group(SAG) for Y2K testing. Other members are the Naval Oceanographic Command, the Air Force Weather Agency, and the FAA. The SAG members participated in two highly successful end-to-end tests with all clients and partners in late January early February 1999 and again in late March and early April 1999.

NOAA reports monthly on the NWS/NESDIS high impact weather program and is publicizing its Y2K readiness in a series of public events throughout the summer and fall of 1999.

*Telecommunications:* NOAA worked closely with the Department's Office of Telecommunications Management to issue a telecommunications assessment of NOAA telecommunications assets. The telecommunications assessment was developed by the Institute for Telecommunications Sciences (ITS) of the National Telecommunications and Information Administration in cooperation with DOC. NOAA and DOC worked closely in formatting the assessment contents to more directly reflect those assets in NOAA. The assessment included telecommunications services such as, voice and data, cellular, satellite, broadcast, multimedia, public access, and Internet capabilities within NOAA. The status of the February 1998 survey from of the DOC Office of Telecommunications Management was that (1) DOC had covered 80% of DOC's telecommunications assets in its inventory and had identified where Y2K problems exist or have been fixed; (2) the remaining 20% are field locations, such as the ASCs and fisheries locations; and (3) both Washington Interagency Telecommunications Systems

(WITS) and FTS 2000 were not Y2K compliant. WITS and FTS 2000 are GSA provided commercial contract telecommunications services to Federal agencies throughout the United States. GSA is reporting that WITS was fixed in July 1998 for Y2K compliance. Voice mail obtained from WITS is already Y2K compliant. FTS 2000 will be replaced by FTS 2001, a Y2K compliant system. In doing contingency planning, we are to assume that they do not work. . . . .

As of March 31, 1999, the status of the telecommunications services by OFA is the following for:

Washington Metropolitan Area: OFA has completed its assessment of the telephones and voice mail systems for Y2K compliance. Findings were that the telephones are Y2K compliant and a voice mail system's Y2K compliancy is dependent on its make and model. For those voice mail systems that were found to be non Y2K compliant (43), they are either being upgraded or replaced. As of July1999, telephone request orders have been received to have 35 voice mail systems upgraded for Y2K compliance.

The ASCs: They have completed conducting assessments of their telephones, voice mail systems and fax machines for Y2K compliance. Primary findings are that the telephones are Y2K compliant and the voice mail systems are not. EASC has an Octel voice mail system. MASC telephones are managed by the National Institute of Standards and Technology (NIST) and not NOAA. NIST is reporting that the voice mail systems are not Y2K compliant. An upgrade is being ordered to take care of that. CASC resides in a GSA-controlled building and uses a switch owned by GSA. The CASC's Meriden key system is Y2K compliant. The Norstar Voicemail was upgraded in 1998 to a model 8 for Y2K compliant. The Cisco 2501 router BIOS upgrade was purchased in September 1998 and CASC is waiting on the contractor to install the upgrade. The fax machines and copiers are Y2K compliant. One fax will require the date to be manually reset after January 1, 2000. WASC telephone system (PBX) is owned by GSA and operated by US West. WASC has received certification from both parties on Year 2000 compliancy. Upgrades for WASC's voice mail system (Octel/Aspen model 4.12A) and fax server have been made and manufacture certifications are on file. NOAA WAN and Internet connectivity is provided to WASC by other components within NOAA. They are taking care of the certification of this equipment (routers) and related software/firmware. All the other telecommunications equipment (multiplexer, CSU/DSU, modems) have manufacturer certifications on file.

*Independent Verification and Validation:* NOAA continues to evaluate its IV&V requirements. NOAA will use a combination of in-house Quality Assurance Teams, outside contract support, and, where possible, DOC or OIG validation processes. NOAA has recommended most of NWS' and NESDIS' systems for IV&V by the Department of Commerce contractors. Both NWS and NESDIS also will depend on the end-to-end test for much of its IV&V effort.

All NOAA Offices have rigorous Configuration Management processes in place. These preceded the Y2K effort. The Year 2000 concern is another contingency that is being folded into the overall process Configuration Management and Crisis Management processes.

*Regulatory Review.* All of NOAA's regulations are in the National Marine Fisheries Services area. These are related to catch limits, restricted fisheries areas, and protected species and have no Y2K implications in and of themselves. It is not possible to restrict them, but NOAA will continue to review them to ensure that they do not have Y2K implications or affect the readiness of operationally compliant systems.

## 1.1 Purpose

The purpose of this Plan is to ensure the continuity of NOAA's core business processes by identifying, assessing, managing and mitigating year 2000 risks. NOAA's Year 2000 Business Continuity and Contingency Plan (BCCP) will help mitigate the risk that its automated systems are unable to recognize year 2000 dates. Resources critical to operating NOAA's core business processes and key support processes, defined later in this document, are identified so that a basic level of services can be provided to NOAA's customers until the normal level of services can be restored. The BCCP identifies risks and threats, establishes mitigation strategies for the identified risks and threats, and provides contingencies in the event risk mitigation efforts fail.

The NOAA's primary approach to assuring that its mission-critical automated information systems can accommodate the century date change is through replacing, repairing, and retiring various components of its information technology infrastructure. Progress toward complete year 2000 compliance is being monitored closely. NOAA has taken steps to ensure that all legacy system renovations and replacement systems are in production during 1999. Although these efforts greatly reduce the chance of a system failure, there are no guarantees that automated systems will not be adversely affected. NOAA is working closely with its data exchange partners and is monitoring the work of other external organizations to help ensure these systems and services will be available. The BCCP will mitigate the risk that business processes will not be able to operate in the event of an unexpected system failure. This BCCP also will be a fundamental linchpin in NOAA's emerging Critical Infrastructure Assurance process and plans.

## 1.2 Use and Scope

The successful operation of NOAA's core business processes depends heavily upon the uninterrupted operations of its mission-critical automated information systems and the supporting information technology infrastructure. The BCCP will be used to help assure that NOAA's core business and corporate processes remain the central focus in preparing its automated systems for the year 2000. This high level plan identifies broad areas of risk and general mitigation strategies and contingencies. For each core business process and key support process, risk mitigation strategies and contingency plans will work together to ensure that processes continue . As risk mitigation strategies are in place, the degree of risk decreases and the chance for needing to implement the contingency plan are reduced. The BCCP will also be used to identify areas where more detailed plans are needed.

The scope of the BCCP includes the NOAA-wide information technology infrastructure that supports business operations and the mission-critical systems that operate on it. From a business

perspective, potential risks and threats are identified along with risk mitigation strategies. Contingencies also are provided in the event risks and threats are not successfully mitigated. The plan matrices identify the core business processes, as well as telecommunications and facilities, and discusses the strategies to provide for the continuation of a minimum level of critical services.

## 1.3 Roles and Responsibilities

NOAA's Year-2000 Program Coordinator is located in the Systems Acquisition Office and the staff comprising the Y2K Taskforce are located in the Line Offices. Together they have developed a comprehensive year-2000 strategy for the Agency that is being closely monitored for progress and achievement. This team also put together the business continuity and contingency plans. They developed contingency plans for continuing NOAA's business operations in the event of a year-2000 related disruption. This team developed the BCCP by identifying and defining the risks and threats within each core business process and designating the component responsible for dealing with the contingency. It developed risk mitigation strategies and milestones and developed plans for return to normal operations. As team discussions proceeded, it became apparent that local contingency plans needed to be developed and put in place for those components performing a critical role in the core business processes.

## 1.4 Assumptions

In developing the BCCP the following assumptions were made:

- NOAA Offices will be open for business on Saturday, January 1, 2000(weather and emergency related services) and on Tuesday, January 4, 2000 for the full range of business services;
- There is no massive, extended power outage on a national scale; and
- In the event that unexpected system failures occur, NOAA will immediately implement relevant sections of this BCCP.

## 1.5 Methodology

NOAA required each of its Office to analyze it's core business processes and supporting information technology infrastructure to identify risks or threats to providing uninterrupted service. NOAA also required that each Office address its telecommunications and facilities logistical issues for embedded chip or other problems. The Office of NOAA Corps Operations was required to address avionics and ship systems. NOAA then developed individual system contingency plans to be activated should a failure occur. The contingency plans describe the steps NOAA will take to ensure the continuity of the core business processes the automated systems support in the event of a year 2000-induced system failure. In some instances, the contingency refers to business continuity plans developed at the business unit level. The heart of the BCCP is the Risk Mitigation and Contingency Planning matrix that is found in section 2. This matrix will be updated as new and better information becomes available and will be reissued as necessary. The following describes how the NOAA Offices developed the elements of the matrix.

For each core business process, telecommunications, and facilities issue, each NOAA Office determined what areas would be at risk in the event of a Y2K failure. These determinations became the risks and threats. The major systems supporting the processes were also identified.

The business priority is used to determine the most critical areas to which resources should be applied to prepare for a potential failure. It is represented as a numerical score; the highest number reflects the highest priority. The business priority itself derived from two factors, the risk assessment and impact of a failure on NOAA's ability to continue to do business. Risk assessment is the probability that the risk or threat will occur, and is expressed numerically, on a scale of 0 to 1.0. The following factors were considered in determining the risk assessment:

- Whether the system is internal or external to NOAA;
- The number of external influences - dependent on COTS software or hardware, other organizations;
- Whether the system involved new or improved technology;
- The total number of dependent systems and processes; and
- The status of system renovation or replacement.

Because factors such as the status of renovation and replacement will change as time progresses, it is possible that the business priority will change as the year 2000 nears. Thus, the BCCP is an evolving document, and will be updated to reflect new or changed information.

Impact reflects the degree of damage to NOAA's ability to deliver service to its customers if the risk or threat occurs. Impact is expressed as a numeric value in the range of 1 to 10. The higher the value, the more negative the impact on service delivery. Factors contributing to determining the degree of impact are:

- The degree of effect of failure on business operations;
- The scope of the problem and the number of customers who would be affected;
- The effect on the ability to process patent applications, register trademarks, or disseminate information about patents and trademarks; and
- Whether the failure would cause an immediate effect on a customer, a delayed effect, or no effect.

The risk mitigation strategy with corresponding milestone dates and action components are actions to be taken which are designed to eliminate or reduce the impact or likelihood of a risk or threat prior to the time horizon to failure. These are actions that will be taken between now and the time horizon to failure to prevent the threat from occurring.

The contingency and triggers element of the matrix identifies the events that set the contingency plan in motion. Also identified are the levels of critical operations possible in the event of catastrophic failures. The described actions maximize the available functionality and trigger the

activities needed to resume normal operations.

## 1.6 Core Business Processes

NOAA's core business processes depend on a complex infrastructure that is crucial to its ongoing operations. Power, data, and voice telecommunications, along with the Agency's computer operations hardware and software, are essential to ensuring that NOAA's business processes are able to continue uninterrupted. These automated systems are the means by which NOAA is able to provide service on demand to the public, the Agency client population, other government entities, and large and small corporations and individual businesses.

NOAA's strategy for ensuring systems readiness for the Year 2000 centers around the core business processes and the key supporting processes. Planning for business continuity provides a prudent response to critical business risks that cannot be put to rest until all mission-dependent computer systems have been shown to be operationally stable and free of year-2000 problems. The business risks to NOAA stem from the potential failure of both internal and external information and systems.

NOAA has analyzed its core business processes to identify the risks or threats to providing uninterrupted service, and has devised plans to be activated should a failure occur. The risks and threats along with contingency planning measures are presented in section 2 of the BCCP. NOAA's identified Core Business Processes are as follows:

-Provide weather, hydrologic, marine, and climate forecasts, warnings, and analyses(NWS);
-Data Center Services(NESDIS);
-Satellite Operations(NESDIS);
-Satellite Processing(NESDIS);
-Satellite Research(NESDIS);
-Search and Rescue Satellite Aided Tracking(NESDIS);
-Environmental Data System(OAR);
-NMFS Agency Management(NMFS);
-Living Marine Resources Research Regulation(NMFS);
-Sustain Healthy Coast(NOS);
-Promote Safe Navigation(NOS);
-Administrative and Management Information Systems
    -Financial and Administrative Management Systems(All NOAA); and
-Major Infrastructure Systems
    -Telecommunications(All NOAA)
    -Facilities(All NOAA)
    -Avionics and Shipboard Systems(ONCO).

## 1.7 Dependencies

Given full year 2000 compliance of NOAA's automated systems that support business, policy, and corporate processes, the NOAA will still rely on the compliance of other Federal agencies,

foreign entities, and private sector organizations. All commercial-off-the-shelf software must be certified to be year 2000 compliant, and data exchanges outside the NOAA need to be compliant. For example, NOAA relies on the U.S. Department of Agriculture's National Finance Center Federal Financial System for accounting data for its financial system.

Public utilities, over which the NOAA has no control, are vital to continued operations. These include electrical power, water, and telecommunications services, which are essential for basic logistical support. These utilities are no less important than the year 2000 compliance of NOAA's internal systems.

Telecommunications are especially vital to the functioning of all NOAA service programs and is considered part of the Basic Weather Service. A vast and complex system collects and distributes weather data, including analyses, forecasts, and warnings. Most of the system is composed of leased facilities which are designed to deliver observed data to users within NOAA, transmit processed information from one section of the meteorological system to another, and deliver the final product to the user or mass disseminators.

NOAA is greatly encouraged, however. At a recent Y2K telecommunications conference sponsored by the General Services Administration, it was stressed by three senior telecommunications officials from BellCore, the International Telecommunications Union, and the National Telephone Cooperative Association (representing the rural telephone companies) that there is no date processing involved in accessing a phone line. In other words, these officials made assurances that on the switch-over from 1999 to 2000 that a dial-tone would indeed be available and that calls would be routed through the telecommunications system. Any possible Y2K problems affecting telecommunications would be in support areas such as billing, fault detection, maintenance scheduling, alarm monitoring, service orders, etc. While these support areas are important to continued NWS operations, they are not in the same real-time nature as being able to get a call through the system. The same official from BellCore briefed *the Senate* Select Committee on Y2K on the positive nature of the availability of voice lines and dial-tones into the Year2000.

NOAA also has internal dependencies. For example, before weather services can be provided, present weather must be gathered and analyzed; that is the primary goal of NWS data acquisition programs. These data also are used by the National Climatic Data Center of the National Environmental Satellite, Data, and Information Service, by travelers for air and sea navigation and local operations, for short- and long-range monitoring of the environment, and by research laboratories. To gather these data, the NWS relies on a wide variety of stations and observing systems. Surface weather conditions are observed and reported at 1,000 land stations, about 240 of which are staffed by NWS personnel. The NWS Modernization and Restructuring program (MAR) includes the use of Automated Surface Observing System (ASOS) at all Government sites. Observations over the ocean are made by volunteer cooperative observers and transmitted from more than 2,000 ships. The National Cooperative Program consists of about 12,000 cooperative weather stations that provide daily precipitation totals and temperature extremes for climatic, hydrologic, agricultural, and other service programs. From the surface up to about 100,000 feet, profiles of temperature and moisture are determined and reported by meteorological instruments carried aloft by balloons. Geostationary and Polar satellites are used to monitor

weather conditions at, and above, the surface of the earth. NEXRAD radars provide information on the type, extent, intensity, and movement of areas of precipitation, severe thunderstorms, tornadoes, and hurricanes. Observing programs and systems are organized into various network configurations, some providing data almost continuously while others may provide data on a monthly, or even seasonal basis.

## 1.8 Process for Plan Updates

This represents the first update to the BCCP, originally issued on February 24, 1999, and incorporates the latest compliancy status, Day- One Planning status, and recommendations from the Office of the Inspector General on NESDIS' systems and its section of the BCCP. A subsequent update in the late fall is also possible.

## 1.9 Testing the BCCP and Day-One Planning

*Testing the BCCP*. NOAA, as a normal course of business, already has validated and tested the NWS and NESDIS contingency plans. For the remaining NOAA core business processes, NOAA has already begun validating and testing, to the degree possible. As a means of further validation, the BCCP has been distributed widely to NOAA's staff, partners, and customers with the goal of improving further its risk mitigation strategies and contingency backups and workarounds. Each NOAA element will be assembling Emergency Response Teams and specific individual strategies for "day-one" planning.

As is the case with other agencies that are responsible for ensuring the protection of life and property, actual physical testing of the critical NWS and NESDIS business continuity plans and workarounds occurs regularly. Each NWS and NESDIS site has back-up power, multiple communications links, back-up support sites, and on-call support personnel that are routinely put into action whenever there is a natural disaster occurrence or a facilities or communications problem. NOAA is extremely confident that its detailed plans for proven, multiple-active system redundancies in the weather and satellite critical areas are safe, as complete as possible, and provide a prudent strategy for maintaining business continuity.

In the Office of Finance and Administration(OFA), ONCO, and NMFS where manual processes will be used as temporary workarounds if systems fail in the most mission-critical areas, training and documentation are underway.

In the OAR and NOS, due to the highly technical nature of their systems, temporary workarounds will not be possible. However, in the unlikely event of Y2K system failures, their Emergency Response Teams will perform triage, repair, retest, and bring the systems back on line as soon as possible. In the interim, all partners and customers will be alerted and kept continuously advised of current system status.

Currently, NOAA has two BCCPS–the NOAA Master Plan and a specific BCCP for the NOS' ADS-Client Server System which failed to meet the March 31, 1999, implementation date and is scheduled for a September 30, 1999 implementation. Further testing exercises are planned during the August/September 1999 time frame and the need for further day-one planning and

additional BCCPs will be assessed at that time.

*Day-One Planning.* *Millennium Rollover and Leap-Year Strategies (**NOTE: Same strategy to be used for February 28-29, 2000)***

1. A coordinated communication network will be firmly established in the summer of 1999 to include all mission-critical team leads, Emergency Response Teams, Line Office(LO) Y2K leads, NOAA's Y2K Coordinator, senior LO management, Senior NOAA management, specified elements of DOC, and data partners and users. Each Line Office and the NOAA Y2K Coordinator will takes steps to establish and staff a "Y2K Operations Center" which will be operational on December 30, 1999 and will be staffed effective 4:00pm Eastern Standard time on December 31, 1999. It then will be the focal point of communications among all parties on all Y2K status issues. The Centers shall remain operative until all millennium rollover assessments are complete and the Under Secretary gives specific direction to stand down, or until late afternoon January 01, 2000, whichever comes first.

.

2. All mission-critical team leads will call Line Office Y2K lead with individual system results of first date crossing into 2000. These are the 24x7(twenty four hours a day seven days a week) weather related systems NOAA identified in the Business Continuity and Contingency Plan(BCCP) as essential to provide business continuity and will include critical telecommunications and facilities where applicable. The initial reports will be due to the LO Operations Centers within 2 hours of the first critical date crossing. The LO Y2K leads will then transmit the results to the NOAA Y2K Coordinator who will contact the Under Secretary, Deputy U/S, CFO, and CIO. Specified elements of the DOC will be notified of results within 4 hours of the date crossing. ***Note: Weather observations and forecasts are based on Coordinated Universal Time(UTC) which is also referred to as Greenwich Mean Time. This allows weather observations and forecasts the world over to have the same time stamp. Since midnight UTC occurs at 7:00pm Eastern Standard Time(EST) on December 31, 1999, NWS Headquarters along with the six NWS Regional Headquarters Offices will begin to monitor at 4:00pm EST to be fully prepared. After this meteorological New Year passes, and all NWS systems continue to work, NWS will continue to monitor local New Years that will roll in from 11:00pm EST in Puerto Rico, to midnight EST, to 1:00am EST in the Central Time Zone, all the way to 5:00am EST for Hawaii. This extra monitoring is not so much for NWS systems as it is to monitor local infrastructures, such as the performance of utility companies. As an aside, Guam will experience local midnight at 9:00am EST on December 31, 1999, and will give us our first Y2K data point and what we can expect. This is the only NWS location where local New Year occurs before Meteorological New Year at 0000 hours UTC.***

3. If each LO reports Mission Critical Systems are functioning smoothly, the Operational Emergency stand down will be declared by the Under Secretary.

4. If a failure sufficient to impact the mission of any LO is encountered, an Operational Emergency for that LO will be declared by the Under Secretary and the LOs affected will activate the business continuity plans outlined in the BCCP and assemble the Emergency Response Teams to begin immediate remediation.

5. Affected LOs will alert their data partners and users of Y2K problems and plans for the provision of basic, critical services as outlined in the BCCP within 4 hours of system failures.

6. Hourly status reports will be provided by the affected LO Y2K Coordinator to the NOAA Y2K Coordinator who will keep NOAA senior management and DOC elements apprized of ongoing progress.

7. The 24x7 LOs will begin remediation immediately upon detection. The non 24x7 LOs will begin triage on their systems and begin immediate remediation on January 3, 2000. Status reports are due to the Operations Centers within 4 hours of the resumption of normal business operations.

8. On January 5, 2000, a comprehensive Y2K compliance assessment will be undertaken for all systems and a report will be prepared by the LO Y2K lead and transmitted to the NOAA Y2K Coordinator. The NOAA Y2K Coordinator will apprize NOAA senior management and the DOC of overall status.

9. A weekly reporting process, including partners and users of NOAA data, will be established until all systems are functioning normally.

NOAA's Line Offices are close to finalizing individual plans based on unique program concerns and preliminary guidance from the Department on its Day-One Plan. The NOAA Day-One Plans will be updated as necessary to accommodate the future actions of the Federal Information Coordination Center(ICC) and subsequent changes to the Department Plan.

## 2.0 Risk Mitigation and Contingency Planning Matrices

Some mitigation strategies are fundamental to all programs. These include:

-Identify data exchange issues(completed);

-Conduct outreach and awareness efforts(continuous);

-Complete testing and implementation(ongoing);

-Conduct Independent Verification and Validation(ongoing);

-Develop Business Continuity and Contingency Plan(continuous);

-Establish emergency response teams and plans(ongoing); and

-Report progress(continuous).

The individual Office matrices that contain, core business processes, impacts, mitigation strategies, and contingency plans follow.

**1414Core Business Process (CBP):Administrative and Management Information Systems**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.1.1 | NOAA/OFA automated systems for administrative functions such as finance and commitment tracking operations are inoperable due to Year 2000 related problems with automated system. The NOAA Financial Management System (FIMA), Financial Analysis and Commitment Tracking System (FACTS) and NOAA Payment System (NPS) are major automated systems supporting the administrative process. | 01/03/2000 | .2 | 3 | .6 | a) Complete renovation of administrative systems software. | Completed | System Division | 1) In the event automated systems FIMA , FACTS , or NPS are unable to provide automated support to administrative systems due to critical Year 2000 date problems, the application developer/maintenance person will analyze the problem, make corrections and retest immediately. |
| | | | | | | b) Confirm Year 2000 compliance of all vendor software products utilized in automated systems. | Completed | System Division | 2) Automated processing of administrative systems will be suspended as appropriate until corrections are made. |
| | | | | | | c) Complete forward date, integration testing of all administrative automated systems. | Completed | System Division | 3) OFA/ISO will implement the system continency plan. There are several weeks before it becomes critical for payment processing. The fallback for payments will be the manual preparations of checks |

**Core Business Process (CBP):Administrative and Management Information Systems**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.1.2 | OFA management information systems are inoperable due to Year 2000 related problems. The NOAA correspondence system and the Consolidated Logistic System (CLS) are examples. | 01/03/2000 | .2 | 3 | .6 | a) Complete renovation of all administrative systems software. | Completed | System Division and NLSC and ASCs | 1) In the event automated systems such as the correspondence control system and CLS are unable to provided support due to critical Year 2000 date problems, the application developer/maintenance person will analyze the problem, make corrections, and retest immediately. |
| | | | | | | b) Conform Year 2000 compliance of all vendor software products utilized in automated systems. | On going | | 2) Automated processing of MI systems will be suspended as appropriate until corrections are made. |
| | | | | | | c) Complete forward date, integration testing of all administrative automated systems. | 03/31/1999 | System Division and NLSC and ASCs | |

**Core Business Process (CBP): Major Infrastructure Systems**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.1.3 | OFA's Computer Center is not operational. - OFA relies on the Alpha computers to process its various administrative functions. Without the computer center or its backup facility, OFA automated systems are not functional. Problems with this system must be corrected before core administrative functions can fully be processed. | 01/01/2000 | .2 | 5 | 1.0 | a) Confirm Year 2000 compliance of all vendor hardware and software products. | Completed | Computer Division (a-d) | 1) If the Computer Division experiences an extended outage at the Landover facility, implement the Backup and Recovery Plan. |
| | | | | | | b) Review the Backup and Recovery Plan to ensure it is current and enforceable. The Landover facility has a backup and recovery plan to guide it in the event of a major outage. This plan, updated annually, defines the steps necessary to re-establish OFA's critical data processing and telecommunications capabilities at a commercial backup facility. | 10/31/1998 | | 2) If outages are experienced at both the Landover facility and its backup facility, implement the Computer Y2K Contingency Plan and hold data until one of the facilities are restored. |
| | | | | | | c) Check and test backup systems. | 01/31/1999 | | 3) In the event of line failure, the Computer Division will re-route telecommunications lines. |
| | | | | | | d) Monitor telecommunications lines via Network Monitoring Software. | On-going | | |

**Core Business Process (CBP): Major Infrastructure Systems**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.1.4 | Data Telecommunications Outage - NOAA/OFA's automated administrative work would not function without data telecommunications. The Metropolitan Area Network and Internet access are examples of data telecommunications services. Outages must be corrected before core business can be fully processed. | 01//01/2000 | .2 | 10 | 2.0 | a) Review plans to address actions for data telecommunications outages to ensure they are current and enforceable. | 12/31/1998 | Computer Division and Network Operations Center (NOC) | If OFA experiences data telecommunications outages, implement the OFA disaster-recovery plan. There is no redundant path. We will wait for the vendor to repair the line/hardware. |
| | | | | | | b) Check and test backup systems. | 01/31/1999 | | |

**Core Business Process (CBP): Major Infrastructure Systems**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.1.5 | Voice Telecommunications Outage - NOAA/OFA would not be able to communicate with its customers and within NOAA | 01/01/ 2000 | .2 | 10 | 2.0 | a) Request vendor verification of Year 2000 compliance, apply patch, or introduce upgrade to ensure compliance.<br>b) Provide GSA a list of NOAAY2K Critical WITS numbers for testing for continuous operations | 03/31/1999<br>08/16/1999 | System Div/ Telecom& ADP Security Br. | Examine the practicality of cellular/wireless communications. |
| 2.1.6 | Facility infrastructure is inoperable due to systems not being Year 2000 compliant - Many of NOAA/OFA's buildings utilize automated systems for such things as security, environmental control, and elevators, etc. Date sensitive systems not made Year 2000 compliant risk being inoperable January 1, 2000. | 01/01/ 2000 | .1 | 10 | 1.0 | a) Complete the OFA facility surveys. | 03/31/1999 | AGFS/FMD | 1) In the event of a building infrastructure system failure, manual overrides will be applied until system corrections can be made. |
| | | | | | | b) Participate with GSA to use vendor supplied information to check status of vendor products supporting automated infrastructure systems. | Ongoing | AGFS/FMD | 2) OFA will divert resources to ensure corrections are made as soon as possible. |
| | | | | | | c) Develop contingency plans for Washington DC buildings and ASCs, | 03/31/1999 | AGFS/FMD | |

**Core Business Process (CBP): Major Infrastructure Systems**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| | | | | | | d) Identify manual overrides or alternative systems for building infrastructure systems as part of assessment and certification. | 03/31/1999 | AGFS/FMD | 3) Implement backup generators for power outages for critical systems. |
| | | | | | | e) Test infrastructure systems January 1, 2000 to resolve any problems prior for business January 3, 2000. | 06/30/1999 | AGFS/FMD | |

**Mission-Critical Systems(MCS): Office Automation**

| MCS # | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.2.1 | Office Automation applications cease to function. - Routine and high priority plans and correspondence would be disrupted. | 01/01/2000 | .4 | 10 | 4.0 | IT staff report to work 01/01/2000 to test, evaluate, and compensate. | 01/01/2000 | Local IT Staff | IT staff report to work 01/01/2000 to reassess, repair, retest, and implement. Revert to manual processes in the interim. |

**Mission-Critical Systems(MCS): Data Acquisition/Data Processing Systems (aircraft)**

| MCS # | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.2.2 | Onboard data acquisition systems and land based data processing systems fail to function. | 01/01/2000 | .1 | 10 | 1.0 | Aircraft support personnel test and evaluate system performance. | 01/03/2000 | Aircraft Operations Center systems support staff | a) Aircraft Operations Center team analyze the problem, make repair and retest immediately.<br>b)Utilize less sophisticated and non-date sensitive data gathering components to collect data for post processing.<br>c) Deploy other aircraft with systems that remain operative. |

**Mission-Critical Systems(MCS): Scientific Computer System (shipboard)**

| MCS # | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.2.3 | Shipboard data acquisition system logs incorrect year, or system fails to function. | 01/01/2000 | .1 | 10 | 1.0 | All ships are scheduled to be in port and not conducting critical operations. Ships force test and evaluate system performance. Systems support personnel create reformatting procedure to correct the year entry in data fields. | 01/01/2000 | Local ships force | Test, evaluate, retest, install changes. |

**Mission-Critical Systems(MCS): Imaging**

| MCS # | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.2.4 | Document input system or document storage/retrieval system cease to function. | 01/01/2000 | .1 | 10 | 1.0 | Postpone image scanning until problem is repaired. | 01/03/2000 | IT Staff and Vendor on support contract | a) Scan documents and retain on disk file in raw data format for processing when problems are resolved.<br>b) In close contact with vendor, test, resolve, re-test, install changes. |

**Non-Mission-Critical Systems(Non-MCS): Aircraft Avionics**

| Non-MCS # | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.2.5 | Onboard aircraft avionics give misleading flight data or cease to function. | 01/01/2000 | .1 | 10 | 1.0 | Ground aircraft depending on severity of problem. | 01/03/2000 | Aircraft Operations | Deploy other aircraft with less sophisticated avionics that are not date sensitive. |

**Non-Mission-Critical Systems(Non-MCS): Shipboard Systems**

| Non-MCS # | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.2.6 | Shipboard engine room control and monitoring, navigation, security, and environmental, systems provide faulty status report dates. | 01/01/2000 | .1 | 2 | .2 | All ships are scheduled to be in port and not conducting critical operations. | 01/03/2000 | Chief Marine Engineer | Manually control and monitor systems and adjust report dates manually. |
| | | | | | | Identify and contact contractor to assist in evaluation and conduct end-to-end test of all functions and reports by rolling the clocks forward. | 02/28/1999 | | |

**Non-Mission-Critical Systems(Non-MCS): Telecommunications**

| Non-MCS # | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.2.7 | Voice Telecommunications Outage - ONCO would not be able to communicate with its customers. | 01/01/2000 | .1 | 10 | 1.0 | Request vendor verification of Year 2000 compliance, apply patch, or introduce upgrade to ensure compliance. | 01/03/2000 | Local IT staff | Examine the practicality of cellular/wireless communications. |

**Non-Mission-Critical Systems(Non-MCS): Facilities**

| Non-MCS # | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.2.8 | Facility infrastructure is inoperable due to systems not being Year 2000 compliant - A small number of ONCO's buildings utilize automated systems for such things as security, environmental control, and elevators, etc. Date sensitive systems not made Year 2000 compliant risk being inoperable January 1, 2000. | 01/01/2000 | .1 | 10 | 1.0 | a) Participate with NOAA's Facilities Management Division to use vendor supplied information to check status of vendor products supporting automated infrastructure systems. | 12/31/1998 | Local Building Facility Manager (a-d) | a) In the event of a building infrastructure system failure, manual overrides will be applied until system corrections can be made.<br><br>b) ONCO will divert resources to ensure corrections are made as soon as possible. |

**Non-Mission-Critical Systems(Non-MCS): Facilities**

| Non-MCS # | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| | | | | | | b) Develop local contingency plans for Silver Spring building and Field Locations | ongoing | | |
| | | | | | | c) Identify manual overrides or alternative systems for building infrastructure systems under ONCO control. | 12/31/1999 | | |
| | | | | | | d) Test infrastructure systems January 1, 2000 to resolve any problems prior to business January 3, 2000. | 01/01/2000 | | |

National Oceanic and Atmospheric Administration
Business Continuity and Contingency Plan
# NATIONAL WEATHER SERVICE (NWS)

**Core Business Process (CBP):** Provide weather, hydrologic, marine, and climate forecasts, warnings, and analyses Updated 11/9/1999

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| **2.3.1** | NWS is unable to obtain current observational data - 1) surface, radar, upper air, and ship observations, 2) satellite products, 3) weather reconnaissance aircraft. | 01/01/2000 | .1 | 10 | 1.0 | a) Identify existing communications paths and isolate weak links (inventory) | Ongoing | OM<br>OH<br>OSO<br>NCEP<br>Regions<br>Field<br>Offices | 1) Utilize existing emergency communications links and backup plans already in place for maintaining continuity of data and product flow between NCEP & NWSTG, NESDIS, DOD and FAA. If necessary acquire Hydrometerological Automated Data System (HADS) from cooperative groups via internet |
| | | | | | | b) Complete comprehensive system training to ensure compliance | Complete | | 2) Utilize data from backup UPPER AIR units where necessary. |
| | NOTES:<br>1) NEXRAD and ASOS assessed Y2K compliant and did not require repairs - Y2K outages for either of these very unlikely. | | | | | c) Participate in NWS End-to-End test to ensure compatibility with entire network | Complete | | 3) Run models with diminished accuracy with existing data. Models can run with NO new data for a 12-hour production cycle. |

**Core Business Process (CBP):**Provide weather, hydrologic, marine, and climate forecasts, warnings, and analyses

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| | | | | | | d) Document NEXRAD Radar Coverage and identify first and second order backup units in the event of an isolated NEXRAD failure | Complete | | 4) ASOS Failure - Use existing manual observation procedures.<br>5) NEXRAD Failure - utilize data from existing national backup radar site plan. |

**Core Business Process (CBP):** Provide weather, hydrologic, marine, and climate forecasts, warnings, and analyses

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.3.1 (cont) | NWS is unable to obtain current observational data -1) surface, upper air, and ship observations, 2) satellite products, 3) weather reconnaissance aircraft. | 01/01/2000 | .1 | 10 | 1.0 | e) Parallel backup operations are required for both AWIPS and AFOS products until full implementation of all AWIPS weather service offices is complete, some time after January 1, 2000. | Ongoing | | 6) Local telecommunications outages: Utilize data from stations that are NOT experiencing problems to fill in for regions where stations are reporting. |
| | NOTES: 2) NCEP frequently experiences temporary interruptions in input data -- in the event of a Y2K-related outage NCEP will address these outages in the same fashion that it does today. | | | | | f) Cooperative support between NCEP, the Navy's Fleet Numerical Meteorological Operations Center (FNMOC), and the Air Force Weather Agency (AFWA) has existed for some time in terms of data sharing, providing model input and output, comparing model performances, and providing backup support. Support from NOAA's FSL is also available for the RUC2 forecast system; and from the UKMET, ECMWF and Canadian Met Offices for the NCEP ensemble forecasts. | Ongoing | | 7) Loss of NESDIS data ONLY: Normal production will continue with degraded accuracy - notify customers. |

**Core Business Process (CBP):**Provide weather, hydrologic, marine, and climate forecasts, warnings, and analyses

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| | 3) ASOS failure procedures documented in NWS Observing Handbook, Chapter 7, Part 3. | | | | | | | | 8) Loss of NWS data ONLY: Forecast accuracy degraded to a greater extent than in 7 - same action. |
| | | | | | | | | | 9) Primary backup to produce analysis and forecast parameters is FNMOC and AFWA, per interagency agreement, and with NOAA FSL per MOA. |

# National Oceanic and Atmospheric Administration
# Business Continuity and Contingency Plan
# NATIONAL WEATHER SERVICE (NWS)

**Core Business Process (CBP):**Provide weather, hydrologic, marine, and climate forecasts, warnings, and analyses

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.3.2 | NWS is unable to produce the suite of forecast products due to 1) failure to receive data, 2) hardware or software failures, or 3) breakdown of communications | 01/01/2000 | .1 | 10 | 1.0 | a) Complete renovation of forecast models. | Complete | NCEP NWSRFS (a-j) | 1) Utilize emergency communications links and backup plans already in place for maintaining continuity of data and product flow between NCEP & NWSTG, NESDIS, DOD and FAA. |
| | NOTE: Does not assume a catastrophic outage; NWS has real time experience with short term outages and working with emergency services. | | | | | b) Participate in the NWS End-to-End test to validate data ingest capability. | Complete | | 2) NCEP frequently experiences temporary interruptions in input data - in the event of a Y2K-related interruption NCEP will address the interruption in the same way that it does today: run models with diminished accuracy on the data available. Models can run with *no* new data for several 12-hour production cycles - with progressive decline in accuracy. |
| | | | | | | c) Complete testing of forecast models with forward dates set on all system components. | Complete Class VII Class VIII | | 3) Hardware failures - utilize one of 3 existing backup systems. |

**Core Business Process (CBP):**Provide weather, hydrologic, marine, and climate forecasts, warnings, and analyses

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| | | | | | | d) Identify existing communications paths and isolate weak links (inventory). | Complete | | 4) Software Failure - mobilize software team to isolate and repair problems. |
| | | | | | | e) Develop communications contingency plan. | 01/31/1999 | | 5) Produce long range (extended) forecasts December 26-31, 1999. |
| | | | | | | f) Complete CLASS VIII Migration efforts with the possible exception of the GFDL Hurricane forecast system that will not be need again until May 2000. | 12/15/1999 | | 6) Utilize Informix Database and Graphical Viewer to produce manual forecasts in the event NWSRFS software fails. |
| | | | | | | g) Implement CLASS VIII System - Delay by FB4(Suitland) facility problems and move to Bowie. Operational products will be disseminated 1/15/2000. | 1/15/2000 | | 7)Class VII will serve as contingency backup if Class VIII is delayed. |
| | | | | | | h) Cooperative support between NCEP, the Navy's Fleet Numerical Meteorological Operations Center (FNMOC), and the Air Force Weather Agency (AFWA) has existed for some time in terms of data sharing, providing model input and output, comparing model performances, and providing backup support. Support from NOAA's FSL is also available for the RUC2 forecast system; and from the UKMET, ECMWF and Canadian Met Offices for the NCEP ensemble forecasts. | Ongoing | | |

# NATIONAL WEATHER SERVICE (NWS)

**Core Business Process (CBP):**Provide weather, hydrologic, marine, and climate forecasts, warnings, and analyses

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| | | | | | | i) Disseminate copies of NWSRFS Y2K Compliant software to RFC sites. | Complete | | |
| | | | | | | j)Upgrade Class VII (C90) operating system for Y2K compliance | Complete | | |

National Oceanic and Atmospheric Administration
Business Continuity and Contingency Plan
# NATIONAL WEATHER SERVICE (NWS)

**Core Business Process (CBP):Provide weather, hydrologic, marine, and climate forecasts, warnings, and analyses**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.3.3 | NWS is unable to disseminate products.<br><br>NOTE: AFOS is not affected by Y2K and is Leap Year ready. | 01/01/2000 | .1 | 10 | 1.0 | a) Conduct extensive system testing to isolate Y2K problems. | Ongoing | OSO<br>NESDIS<br>AWIPS<br>GSA | 1) AWIPS Failure: Utilize AFOS for data dissemination. |
| | | | | | | b) Continue testing for Y2K compatibility with any and all software releases. | Ongoing | | 2) Utilize existing backup communications links. |
| | | | | | | c) Participate in NWS End-to-End test to ensure integration and compatibility with entire network | Complete | | 3) Make data available on other sources which are accessible where possible, such as web sites, ftp servers, etc. |
| | | | | | | d) Identify existing communications paths and isolate weak links (inventory). | Ongoing | | 4)Utilize DOD's Automated Weather Network (AWN) and DMS circuits as a backup for WMO Global Telecommunications System (GTS). |
| | | | | | | e) Request vendor certification of communications services. | Ongoing | | 5)The AWIPS Communications Network (ACN) will serve as a backup to the NWSTG as necessary. |

**Core Business Process (CBP):Provide weather, hydrologic, marine, and climate forecasts, warnings, and analyses**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| | | | | | | f) Parallel backup operations are required for both AWIPS and AFOS products until full implementation of all AWIPS weather service offices is complete, some time after January 1, 2000. | Ongoing | | 6)If necessary, acquire Hydrometeorological Automated Data System (HADS) from cooperative groups via Internet. |
| | | | | | | g) NWS requires backup communications to receive alphanumeric data from the FAA in the event of an NWSTG failure. | | | |
| 2.3.4 | Voice Telecommuni-cations - Outage impacts ability to communicate within the NWS. | 01/01/2000 | .1 | 1 | .1 | a) Request vendor certification of Y2K Compliance.<br>b) Local carriers have provided documentation of Y2K compliance. | 11/01/1998<br><br>11/30/1998 | OFA/ Systems Division | 1) Utilize cellular phones where possible.<br>2) Vendor has certified that Merlin II Systems are Year 2000 compliant. |
| 2.3.5 | Facility Infrastructure - Outage affects access and use of the facility. | 01/01/2000 | .1 | 2 | .2 | a) Work with GSA to use vendor supplied information to check status of vendor products supporting automated infrastructure systems. | Ongoing | GSA NOAA NWS Regions Facility Manager (a-c) | 1) Implement manual overrides for automated system failures. |
| | | | | | | b) Request vendor certifications for leased sites. | Ongoing | | 2) Implement backup generators for power outages. |

**Core Business Process (CBP):Provide weather, hydrologic, marine, and climate forecasts, warnings, and analyses**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| | | | | | | c) Identify manual overrides or alternatives systems for building access systems as part of assessment and validation efforts. | Ongoing | | 3) Re-site the hydrologic forecast process in the Silver Spring facility if infrastructure failures occur at an RFC |

**Core Business Process (CBP): Environmental Data System**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Risk Mitigation Strategy | Milestone Dates | Action Component | |
| 2.4.1 | OAR is unable to provide environmental information and data to its customers | 01/01/2000 | .2 | 10 | 2.0 | a) Identify all data exchange partners and establish Memoranda of Agreement as necessary. | Completed | System Developers | 1) In the event that OAR's mission critical systems are unable to function the emergency response team will analyze the problem, make repair, and retest immediately. Two categories of "Triggers" have been identified: |
| | | | | | | b) Continue outreach and awareness efforts with customers and partners. | Ongoing | | a) Catastrophic failure: This is defined as systems halt or hang at the operating system or hardware level; required subsystems crucial to operations fail to start or run. A failure of this nature would most likely be solved by setting the system time back to some corresponding date in 1990, and identifying, changing and testing all necessary software to compensate for the 10 years of difference. |
| | | | | | | c) Complete renovation of mission critical systems: FSL Wind Profiler; and Space Weather System. | 09/30/1998 | | b) Fatal failures: defined as the applications software halts or fails to perform as currently defined. These we can identify and fix as needed, having access to the source code. |

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Risk Mitigation Strategy | Milestone Dates | Action Component | |
| | | | | | | d) Develop validation test plan. | 11/15/1998 | | 2) Data delivery to OAR's customers will be suspended until corrections are made. |
| | | | | | | e) Develop Business Continuity and Contingency Plan. | 11/15/1998 | | |
| | | | | | | f) Establish IV & V Team. | 11/30/1998 | | |
| | | | | | | g) Assign emergency response team in anticipation of system failure. | 11/30/1998 | | |
| | | | | | | h) Coordinate test with data exchange partners; determine point-of-contact with external organizations; meet formally and determine points of failure, establish test procedures and schedule "live" test where practical and permitted. | 12/15/1998 | | |
| | | | | | | I) Prepare simulated data input where necessary and feasible. | 12/15/1998 | | |
| | | | | | | j) Complete testing with forward dates set on all system components. | 01/31/1999 | | |
| | | | | | | k) Implement System. | 03/31/1999 | | |
| | | | | | | l) Continue reporting progress and highlighting problems and successes. | Ongoing | | |

**Core Business Process (CBP): Financial Management System**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.4.2 | OAR is unable to process financial transactions electronically (data entry and reporting) | 01/01/2000 | .1 | 7 | .7 | a) Continue outreach and awareness with customers and partners. | Ongoing | LASS Team (a-k) | 1) In the event that OAR's financial system fails the emergency response team will analyze the problem, make correction, retest and redistribute software. |
| | | | | | | b) Complete renovation of financial management system. | 09/30/1998 | | 2) Data entry will be accomplished through standard Government paper forms which will be entered electronically after system corrections are made. |
| | | | | | | c) Develop validation test plan. | 11/15/1998 | | 3) Financial reporting will be suspended until system corrections are made, or reports will be generated from the FIMA system. |
| | | | | | | d) Develop Business Continuity and Contingency Plan. | 02/15/1999 | | |
| | | | | | | e) Establish IV & V Team. | 11/30/1998 | | |
| | | | | | | f) Assign Emergency Response Team in anticipation of system failure. | 11/30/1998 | | |
| | | | | | | g) Conduct data entry testing with forward dates set on all system components. | 01/31/1999 | | |
| | | | | | | h) Prepare simulated FIMA data input for FY 2000. | 01/31/1999 | | |

**Core Business Process (CBP): Financial Management System**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| | | | | | | I) Conduct data reporting testing using simulated FIMA data and manually entered FY 2000 data. | 01/31/1999 | | |
| | | | | | | j) Implement System. | 03/31/1999 | | |
| | | | | | | k) Continue reporting progress and highlighting problems and successes. | Ongoing | | |

# OFFICE OF OCEANIC AND ATMOSPHERIC RESEARCH (OAR)

**Core Business Process (CBP): Facilities**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.4.3 | Facility components fail to operate as expected; security systems, elevators, environmental controls fail. Facility access is hindered. | 01/01/2000 | .1 | 10 | 1.0 | a) Inventory OAR facilities and communicate findings to NOAA Y2K and OFA facilities coordinator. | 11/15/1998 | Facility Manager (a-d) | 1) In the event of a building infrastructure system failure, manual overrides will be applied until system corrections can be made. |
| | | | | | | b) Determine Y2K compliance level of Facilities systems, including elevators, security, HVAC, fire, etc. | 12/15/1998 | | 2) Facility managers will work with building maintenance personnel to ensure continued operations and to correct deficiencies. |
| | | | | | | c) Renovate non-compliant facility components. | 03/31/1999 | | |
| | | | | | | d) Assign emergency response team. | 06/30/1999 | | |

**Core Business Process (CBP): Telecommunications and Networks**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.4.4 | Telecommunications Fail - OAR is unable to communicate via phone system. | 01/01/2000 | .1 | 10 | 1.0 | a) Inventory OAR phone systems and | 11/15/1998 | Phone System Managers (a-d) | 1) Phone systems fail - consider cost effectiveness of cellular / wireless communications and/or e-mail until problems are resolved. |
| | | | | | | b) Determine Y2K compliance level of phone and voice mail systems. | 12/15/1998 | | |
| | | | | | | c) Renovate non-compliant systems. | 01/31/1999 | | |
| | | | | | | d) Assign emergency response team. | 06/30/1999 | | |
| 2.4.5 | LAN, MAN, or Internet services fail - OAR is unable to communicate or provide data to its customers. | 01/01/2000 | .2 | 5 | 1.0 | a) Inventory OAR Network Equipment. | 11/15/1998 | Network Managers (a-d) | 1) OAR networks fail - cease operations until corrections are made. |
| | | | | | | b) Determine Y2K compliance level of network devices. | 11/15/1998 | | |
| | | | | | | c) Renovate non-compliant network equipment. | 03/31/1999 | | |
| | | | | | | d) Assign emergency response team. | 06/30/1998 | | |

# National Oceanic and Atmospheric Administration
# Business Continuity and Contingency Plan
# NATIONAL OCEAN SERVICE

**Core Business Process(CBP): Promote Safe Navigation**
**Mission-Critical System(MCS): Automated Distribution System (ADS) and Aeronautical Chart Automation System (CONDOR)**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.5.1.1 ADS | Without a working ADS, the automated distribution of nautical and aeronautical charts and related publications would be impaired or interrupted. Without up-to-date charts, the safety of private and commercial navigation and aviation would be jeopardized. | 10/01/1999 | .3 | 10 | 3.0 | Award Contract<br>Contractor deliver Build One of software<br>Contractor deliver Build Two of software<br>Begin user training on SW<br>Contractor deliver Build Three of software<br>Develop ADS BCCP<br>Contractor deliver Final version of software | 12/15/1998<br>05/31/1999<br>06/18/1999<br>06/21/1999<br>07/08/1999<br>07/16/1999<br>07/28/1999 | ACC<br>ACC<br>ACC<br>ACC<br>ACC<br>ACC<br>ACC | 1 Limited Operation: If the ADS fails partially and the distribution function is working properly, the DD will continue to operate in a limited capacity. Orders will be entered and processed. Financial tracking will be suspended to be resumed at a later date. Paper trails will exist for later account reconciliation. Programmers will make repairs as necessary.<br>2 Partial Operation: If the system cannot function after 01/01/2000, SDG will reset the date on the backup server to the corresponding prior date in the cycle. The system will function, however, DD personnel will be required to make data modifications to compensate for the incorrect dates in the data. Paper trails will exist for data entry at a later date for reconciling accounts. Programmers will make necessary repairs.<br>3. Manual Operaton: If resetting the date on the backup system is unreliable, complete manual operation will begin. Data from the 12/31/1999 small product realease cycle run will beupdated and made available to distribution contractors. Manual update by DD personnel will continue until repairs are made, the system tested, and operational. Updated files will be made available to DD on a daily basis. |

**Core Business Process(CBP): Promote Safe Navigation**
**Mission-Critical System(MCS): Automated Distribution System (ADS) and Aeronautical Chart Automation System (CONDOR)**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.5.1.1 ADS (cont) | | | | | | Acceptance Test Starts<br>Y2K Compliance Test<br>Small Product Release Cycle<br>Final acceptance of software | 08/21/1999<br>09/03/1999<br>09/17/1999<br>09/30/1999 | ACC<br>09/30/1999<br>ACC<br>ACC | 3 Manual Operation (cont) History files for previous product release cycle runs will be consulted for verifying product schedules and subscription information. Paper trails will exist for data entry at a later date for reconciling accounts. Programmers will make needed repairs.<br>4 Existing System Modifications: Modifying the current system is only an option if the new system proves to be unacceptable by 10/01/1999. Programmers will perform the necessary modifications to the programs to continue using the system through 01/01/2000, and until the new system be repaired and is accepted.<br>**Business Resumption**<br>Under any of the failure strategies listed above, teams will be formed to process and deliver orders. The teams will track inventory and accounting information for entry into the system at a later date and after the system is functional. Under failure strategies two, three, and four, AC&C constituents, major Government clients (FAA and NIMA), and the top twenty aeronautical and nautical agents will be notified of the problems. Nearly 80% of the products distributed by AC&C are purchased by these customers. These groups will be alerted of possible order fulfillment problems and asked to notify the DD of any irregularities with their orders. Upon notification of problems, missing products will be shipped to the customer overnight at no additional charge. |

**Core Business Process(CBP): Promote Safe Navigation**
**Mission-Critical System(MCS): Automated Distribution System (ADS) and Aeronautical Chart Automation System (CONDOR)**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.5.1.2 CONDOR | Aeronautical Chart System outage. AC&C is unable to compile aeronautical charts, process source document data and publish aeronautical chart/data publications. | 01/03/2000 | 0.1 | 10 | 1.0 | A. Develop local year 2000 test plan.<br>B. Conduct forward date, integration testing of critical ACC/ACD hardware and software. Evaluate hardware compliance using in-house and 3rd party Year 2000 tools . ACC/ACD's Aeornautical Chart Automation Branch will act as the Business Resumption Team. | 12/31/1998 | ACC/ACD (a-b) | 1) In the event that the automated processing of aeronautical data fails due to Year 2000 date problems, the Business Resumption Team will analyze the problem, make corrections and retest immediately.<br>2) Processing on affected systems will be suspended until corrections are made |

National Oceanic and Atmospheric Administration
Business Continuity and Contingency Plan
# NATIONAL OCEAN SERVICE

**Core Business Process(CBP): Promote Safe Navigation**
**Mission Critical Systems (MCS): Physical Oceanographic Real-Time Systems (PORTS), Currents Data Processing System (Currents), Continuous Operational Real-time Monitoring System (CORMS), Data Processing and Analysis System (DPAS) and Tide and Current Prediction System**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.5.1.3 PORTS | Real time currents, water levels, and winds would not be available to the public in San Francisco, New York, Tampa, Houston and Chesapeake | 01/01/2000 | .1 | 10 | 1.0 | 1. Develop contingency plan. | 02/15/1999 | CO-OPS Chief Information Systems Division; PORTS Operations Manager and Field Operations Division Chief | 1. In the event the DAS and other related PORTS systems are unable to provide real-time observations to the public due to critical Year 2K date problems, the Business Resumption Team will analyze the problem, make corrections and retest immediately. |
| | | | | | | 2. Train local PORTS managers on contingency plan. | 03/31/1999 | | 2. Given a total system failure, PORTS data dissemination will be suspended until corrections are made and a notice placed on the CO-OPS web site. |

**Core Business Process(CBP): Promote Safe Navigation**
**Mission Critical Systems (MCS): Physical Oceanographic Real-Time Systems (PORTS), Currents Data Processing System (Currents), Continuous Operational Real-time Monitoring System (CORMS), Data Processing and Analysis System (DPAS) and Tide and Current Prediction System**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| | | | | | | | | | 3. In the event of a failure of one or more of the sensors used by PORTS, that PORTS will continue to report the available data. The unavailable data will be identified as not available at that time. Only the reference Tides gages used by PORTS have backup sensors. No manual measurements or degraded data sources are available. |

**Core Business Process(CBP): Promote Safe Navigation**
**Mission Critical Systems (MCS): Physical Oceanographic Real-Time Systems (PORTS), Currents Data Processing System (Currents), Continuous Operational Real-time Monitoring System (CORMS), Data Processing and Analysis System (DPAS) and Tide and Current Prediction System**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.5.1.4 CURRENTS | Post processed current meter data and analysis would not be available for use in NOS products. | 02/01/2000 | .1 | 5 | .5 | 1. Develop contingency plan. | 02/15/1999 | CO-OPS Chief Information Systems Division (ISD) | 1. In the event the current processing software and other related current processing systems are unable to provide current post processing and analyses for NOS products due to critical Year 2K date problems, the Business Resumption Team will analyze the problem, make corrections and retest immediately. |
| | | | | | | 2. Train current processing team on contingency plan. | 03/31/1999 | Chief ISD | 2. Current post-processing and analysis of data will be suspended until corrections are made. |
| 2.5.1.5 CORMS | Quality control monitoring of PORTS data would not be performed. | 01/01/2000 | .1 | 10 | 1.0 | 1. Develop contingency plan. | 02/15/1999 | CO-OPS Chief Information Systems Division and OAD Chief | 1. In the event the CORMS software and other related CORMS systems are unable to provide real time monitoring of PORTS data due to critical Year 2K date problems, the Business Resumption Team will analyze the problem, make corrections and retest immediately. |

National Oceanic and Atmospheric Administration
Business Continuity and Contingency Plan
# NATIONAL OCEAN SERVICE

**Core Business Process(CBP): Promote Safe Navigation**
**Mission Critical Systems (MCS): Physical Oceanographic Real-Time Systems (PORTS), Currents Data Processing System (Currents), Continuous Operational Real-time Monitoring System (CORMS), Data Processing and Analysis System (DPAS) and Tide and Current Prediction System**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| | | | | | | 2. Train local PORTS managers and CORMS operators on contingency plan | 03/31/1999 | | 2. CORMS monitoring will be suspended until corrections are made. |

**Core Business Process(CBP): Promote Safe Navigation**
**Mission Critical Systems (MCS): Physical Oceanographic Real-Time Systems (PORTS), Currents Data Processing System (Currents), Continuous Operational Real-time Monitoring System (CORMS), Data Processing and Analysis System (DPAS) and Tide and Current Prediction System**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.5.1.6 DPAS | Water level data from the national water level observation network would not be available to the public. | 01/01/2000 | .1 | 10 | 1.0 | 1. Develop contingency plan. | 09/30/1998 | CO-OPS Chief Information Systems Division and OAD Chief | 1. In the event the DPAS software and other related DPAS systems are unable to provide real time data due to critical Year 2K date problems, the Business Resumption Team will analyze the problem, make corrections and retest immediately. |
| | | | | | | 2. Train water level processors on contingency plan | 03/31/1999 | | 2. Water level data processing and dissemination will be suspended until corrections are made. |

National Oceanic and Atmospheric Administration
Business Continuity and Contingency Plan
# NATIONAL OCEAN SERVICE

**Core Business Process(CBP): Promote Safe Navigation**
**Mission Critical Systems (MCS): Physical Oceanographic Real-Time Systems (PORTS), Currents Data Processing System (Currents), Continuous Operational Real-time Monitoring System (CORMS), Data Processing and Analysis System (DPAS) and Tide and Current Prediction System**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.5.1.7 Tide and Current Prediction System | Predictions for ad hoc queries as well as for NOS products would not be available to the public. | 01/01/2000 | .1 | 8 | .8 | a. Develop contingency plan. | 02/15/1999 | CO-OPS Chief Information Systems Division and OAD Chief (a-b) | 1. In the event the Tide and Current Prediction software and other related systems are unable to provide Tide and Current predictions due to critical Year 2K date problems, the Business Resumption Team will analyze the problem, make corrections and retest immediately. |
| | | | | | | b. Train appropriate personnel on contingency plan | 03/31/1999 | | 2. Tide and Current Predictions dissemination will be suspended until corrections are made. |

# National Oceanic and Atmospheric Administration
# Business Continuity and Contingency Plan
# NATIONAL OCEAN SERVICE

**Core Business Process(CBP): Promote Safe Navigation**
**Mission-Critical System(MCS): Hydrographic Processing System and Nautical Charting System**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.5.1.8 Hydro Proc. System | Hydrographic Surveys Division (HSD) is unable to process hydrographic data. HSD is unable to give adequate instructions to field units, unable to review data submitted from the field, and unable to deliver hydrographic data products to Marine Charting Division. | 01/03/2000 | .1 | 10 | 1.0 | a. Develop local year 2000 test Plan. | 12/31/1998 | HSD (a-c) | 1) In the event HSD is unable to process Hydrographic Data due to critical Year 2000 date problems, the Business Resumption Team will analyze the problem, make corrections, and retest immediately. |
| | | | | | | b. When feasible, conduct forward date, integration testing of critical HSD hardware and software. Evaluate hardware compliance using in-house and 3rd party Year 2000 tools. | 03/31/1999 | | 2) Processing on affected systems will be suspended until corrections are made. |
| | | | | | | c. HSD's System Support Branch will act as the Business Resumption Team. | | | |

**Core Business Process(CBP): Promote Safe Navigation**
**Mission-Critical System(MCS): Hydrographic Processing System and Nautical Charting System**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.5.1.9 Nautical Charting System | Nautical Chart System outage | 01/03/2000 | 0.1 | 10 | 1.0 | a. Develop local year 2000 test Plan. | 12/31/1998 | MCD (a-b) | 1) In the event that the automated processing of nautical data fails due to Year 2000 date problems, the Business Resumption Team will analyze the problem, make corrections and retest immediately. |
| | Marine Charting Division (MCD) is unable to compile nautical charts, process source document data and publish coast pilot publications. | | | | | b. When feasible, conduct forward date, integration testing of critical MCD hardware and software. Evaluate hardware compliance using in-house and 3rd party Year 2000 tools.<br><br>MCD's System Support Branch will act as the Business Resumption Team. | 03/31/1999 | | 2) Processing on affected systems will be suspended until corrections are made. |

National Oceanic and Atmospheric Administration
Business Continuity and Contingency Plan
# NATIONAL OCEAN SERVICE

**Core Business Process(CBP): Promote Safe Navigation**
**Mission-Critical System(MCS): Integrated Data Base (NGSIDB) and Continuously Operating Reference System (CORS)**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.5.1.10 NGSIDB | System Outage - Our customers will be unable to access the NGSIDB system to do their scientific processing, loading of geodetic positional information and the retrieval of the NGS positional information which support the business community throughout the nation. The NGSIDB is supported by a system of NT and UNIX processors. | 01/03/2000 | .3 | 10 | 3.0 | a) Continue the testing of all NGS operating systems, software and systems for Y2K compliance. | 09/30/1998 | NGS (a-b) | 1) In the event NGS Systems are unable to provide automated support to NGS customers due to network Year 2000 date problems, the Business Resumption Team for NGS will analyze the problem, make necessary corrections, retest the network immediately and resume production. |
| | | | | | | Note All NGS data uses a 4 character date field for the year. Because of this formatting NGS software has always used a 4 character year field in their programming and “year 2000" is not a problem for either the data or the NGS developed application programs. | 12/31/1998 | | 2) Processing on affected systems will be suspended until corrections are made. |
| | | | | | | b) Establish a NGS Y2K Business Resumption Team for the NGS systems. | | | |

**Core Business Process(CBP): Promote Safe Navigation**
**Mission-Critical System(MCS): Integrated Data Base (NGSIDB) and Continuously Operating Reference System (CORS)**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.5.1.11 CORS | X.25 Network communications Outage - NGS systems are not functional without FTS2000 network communications . Outages must be corrected by network communication providers before core business can be work. | 01/01/2000 | .2 | 10 | 2.0 | a) Review local plans to address actions for network communications outages to ensure they are current. | 12/31/1998 | NGS (a-b) | 1) If NGS experiences network communications outages at the local level, implement dial-up networking or use any other available provider. |
| | | | | | | b) Review outage strategy with NOAA network communication providers. | 12/31/1998 | | 2) If regional or national level telecommunications outages are experienced, maintain local network until other level of communications are restored. |

# National Oceanic and Atmospheric Administration
# Business Continuity and Contingency Plan
# NATIONAL OCEAN SERVICE

**Core Business Process(CBP): Promote Safe Navigation**
**Mission-Critical System(MCS): Integrated Data Base (NGSIDB) and Continuously Operating Reference System (CORS)**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.5.1.12 CORS | System Outage - Our customers will be unable to access the CORS system to retrieve the available CORS information which support the business community throughout the nation. The CORS is supported by a system UNIX processors | 01/01/2000 | .3 | 10 | 3.0 | a) Develop contingency plans for CORS systems. | 02/15/1999 | NGS | 1) In the event NGS Systems are unable to provide automated support to NGS customers due to network Year 2000 date problems, the Business Resumption Team for NGS will analyze the problem, make necessary corrections, retest the network immediately and resume production. |
| | | | | | | Note. All NGS CORS data uses a GPS week date field for their observations. Because of this formatting NGS CORS software is not effected by the Y2K date and “year 2000" is not a problem for either the data or the NGS developed application programs | | | 2) Processing on affected systems will be suspended until corrections are made. |

National Oceanic and Atmospheric Administration
Business Continuity and Contingency Plan
# NATIONAL OCEAN SERVICE

**Core Business Process(CBP):2.5.2.0 Sustain Healthy Coasts**
**Mission-Critical System(MCS): CSC Support System**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.5.2.1 CSC Support System | Scientific and Business System Outage - CSC is unable to access business systems or process center products such as CCAP, CRS, and GIS products that must be delivered to CSC partners and the public. CSC scientific and business systems are supported by a system of NT and UNIX processors. | 01/03/2000 | .3 | 10 | 3.0 | a) Complete renovations of all CSC software and related systems. | 09/30/1998 | CSC (a-d) | 1) In the event CSC Systems are unable to provide automated support to CSC Scientific and Business Systems due to critical Year 2000 date problems, the Business Resumption Team for CSC will analyze the problem, make corrections, and retest immediately. |
| | | | | | | b) Complete forward date, integration testing of all CSC scientific and business system. | 12/31/1998 | | 2) Processing on affected systems will be suspended until corrections are made. |
| | | | | | | c) Develop local Y2K Contingency Plan. | 12/31/1998 | | |
| | | | | | | d) Establish a Business Resumption Team for the CSC systems. | 12/31/1998 | | |

National Oceanic and Atmospheric Administration
Business Continuity and Contingency Plan
# NATIONAL OCEAN SERVICE

**Core Business Process(CBP):2.5.2.0 Sustain Healthy Coasts**
**Mission-Critical System(MCS): CSC Support System**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.5.2.2 | Facility infrastructure Outage - CSC buildings utilize automated systems for such things as security, environmental controls, and elevators, etc. Date sensitive systems not made Year 2000 compliant risk being inoperable Jan 1, 2000. | 01/01/2000 | .1 | 8 | .8 | a) Develop contingency plans for CSC buildings. | 12/31/1998 | CSC (a-c) | 1) In the event of building infrastructure system failure, manual overrides will be applied until system corrections can be made. |
| | | | | | | b) Identify manual overrides or alternative systems for building infrastructure systems as a part of assessment and certification. | 12/31/1998 | | 2) CSC will divert resources to ensure corrections are made as soon as possible. |
| | | | | | | c) Test and inspect infrastructure systems January 1, 2000 to resolve any problems prior to opening for business January 3, 2000. | 01/01/2000 | | |

**Core Business Process(CBP):2.5.2.0 Sustain Healthy Coasts**
**Mission-Critical System(MCS) : DAC Network and DAC Email**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.5.2.3 DAC Network | DAC staff will no longer be able to perform duties that rely on the DAC Network. (Examples: Modification of shared documents stored on servers, network backups, | 01/01/2000 | .3 | 7 | 2.1 | a) Computers on the DAC network that have hardware barriers to meeting Y2K will be replaced with new computers that are Y2K compliant. | 12/31/1998 | DAC (a-c) | 1) In the event that computers with hardware barriers to Y2K compliance are found on or after Jan 1, 2000, the computers will be replaced immediately. |
| | | | | | | b) Computers with operating systems that do not meet Y2K compliance will be patched or replaced with Y2K compliant OS's. | 01/ 31/ 1999 | | 2) If any operating system or software upgrades are not performed before Jan 1, 2000, upgrades will be applied immediately after a problem is |
| | | | | | | c) Software applications in use by DAC staff that do not meet Y2K compliance will be upgraded. If no upgrade exists, an alternative Y2K application will be chosen. | 03/15/ 1999 | | |

**Core Business Process(CBP):2.5.2.0 Sustain Healthy Coasts**
**Mission-Critical System(MCS) : DAC Network and DAC Email**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.5.2.4 DAC Email | DAC staff will no longer be able to communicate via Email with local co-workers or external contacts. | 01/01/2000 | .2 | 6 | 1.2 | a) Client computers will have their Email client software tested, and upgraded to Y2K compliance | 12/31/1998 | DAC (a-b) | 1) In the event that a client is unable to use Email services on or after Jan 1, 2000, the email client will be patched or upgraded immediately. |
| | | | | | | b) Email server software and hardware components will be tested and upgraded if necessary. | 01/31/1999 | | 2) If Email servers fail to function properly on or after Jan 1, 2000, the server software will be patched or upgraded immediately. |

**Core Business Process(CBP): Telecommunications and Facilities**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.5.3.1 | Voice Telecommunications Outage - impacts ability to communicate within NOS. | 01/01/2000 | .1 | 10 | 1.0 | a)Request vendor certification of Y2K compliance. | 12/31/1998 | OFA (a-b) | 1) Utilize cell phones or satellite phones where possible |
| | | | | | | b) Local carriers have provided documentation of Y2K compliance. | 12/31/1998 | | 2) Vendor has certified that the Merlin II Systems are Y2K compliant. |
| 2.5.3.2 | Facility infrastructure outage affects access and use of the facility. | 01/01/2000 | .1 | 10 | 1.0 | a) Work with GSA to use vendor supplied information to verify status of vendor products supporting automated facility systems. | Ongoing | GSA NOAA Facilities Manager (a-c) | Implement manual overrides for automated system failures. |

**Core Business Process(CBP): Telecommunications and Facilities**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| | | | | | | b) Request vendor certification statements for leased sites. | Ongoing | | |
| | | | | | | c) Identify manual overrides or alternative procedures for building access systems in assessment and validation efforts. | Ongoing | | |

**Core Business Process (CBP):Data Center Services(NCDC)**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.6.1.1 | NCDC is unable to process climate data and service customers with data and products due to Year 2000 related problems with automated systems. Automated systems and associated processing and applications programs are the major automated systems supporting data processing and customer servicing. | 01/01//2000 | .1 | 10 | 1.0 | a) Complete renovation of software and related systems operating in an open system environment (Y2K issues) | 09/30/1998 | NCDC (a-I) | 1) In the event NCDC mission critical systems are unable to function beyond 1 Jan 2000, the response team will analyze the problem, make repair and retest immediately. The NCDC has on-line data services and off-line data services. On-line data services systems will be given highest priority. Response to off-line data services averages 5 working days . Further delay may be incurred until systems corrections are made, retested and implemented. |
| | | | | | | b) Complete forward date validation of software and related systems operating in an open system environment | 01/31/1999 | | |
| | | | | | | c) Complete local contingency plan | 01/31/1999 | | |

**Core Business Process (CBP):Data Center Services(NCDC)**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| | | | | | | d) Complete implementation of migrated applications programs from UNISYS mainframe to open systems environment. | 03/31/1999 | | |
| | | | | | | e) Complete implementation of systems (Y2K issue) operating in an open systems environment | 03/31/1999 | | |
| | | | | | | f) Complete full integration and implementation of migrated and new development systems to replace UNISYS system applications software. | 09/30/1999 | | |
| | | | | | | g) Assign and schedule response team | 09/30/1999 | | |
| | | | | | | h) Verify all on-line data systems and data acquisition systems operating properly | 01/01/2000 | | |
| | | | | | | i) Verify data services applications systems operate properly | 01/03/2000 | | |

**Core Business Process (CBP):Data Center Services(NODC)**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.6.1.2 | NODC is unable to provide Online Data Access or data products to clients | 01/01/2000 | .1 | 10 | 1.0 | a) Identify all data exchange format. | 06/30/1997 | NODC (a-f) | In the event that the data access and retrieval systems are unable to provide automated support to the Online access process, the systems and software team will analyze the problem, make corrections and retest immediately. Automated access of the data system will be suspended until corrections are made. Operations components will implement the Y2K contingency plan.. |
| | | | | | | b) Continue outreach and awareness efforts with customers and partners. | Ongoing | | |
| | | | | | | c) Completed renovation of all of the data access software and related systems.. | 09/30/1998 | | |
| | | | | | | d) Complete forward date, integration testing of the data access software and related systems. | 03/31/1999 | | |
| | | | | | | e) Establish Y2000 Emergency Project Team | 07/31/1998 | | |
| | | | | | | f) Develop local Y2K contingency plan. | 03/31/1999 | | |

**Core Business Process (CBP):Data Center Services(NGDC)**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.6.1.3 | NGDC is unable to process geophysical and related data, and service customers with data and products due to Year 2000 related problems with automated systems. Sun, Networks, PC systems, associated processing software, and applications programs are the major automated systems supporting data processing and customer service. | 01/01/2000 | .1 | 10 | 1.0 | a) Complete renovation of application software and related data systems operating in the NGDC open system environment (Y2K issues). | 09/30/1998 | NGDC Data and System Administrators | 1) In the event that any of the NGDC mission critical systems are unable to function beyond 1/1/2000, the responsible data and or system administrator will determine the nature and severity of the problem. The DA/SA will then assign the appropriate resources for remediation of the problem in relation to the severity and retest immediately. The NGDC has on-line data services and off-line data services. On-line data |
| | | | | | | b) Complete the NGDC Business Continuity and Contingency Plan. | 10/30/1998 | NGDC Y2K Coordinator | service systems will be given highest priority. Response to off-line data services should average 5 working days. |
| | | | | | | c) Complete validation and testing of related operating systems in the NGDC open system environment. | 01/31/1999 | NGDC Systems Administrators | 2)Data delivery to NGDC's customers from the affected system or systems will be suspended until corrections are made. |
| | | | | | | d) Complete implementation of systems operating in the NGDC open system environment (Y2K issues). | 03/31/1999 | NGDC Data and Systems Administrators | |
| | | | | | | e) Verify all on-line data systems and data acquisition systems operating properly. | 12/31/1999 | NGDC Web Administrators | |
| | | | | | | f) Verify data services applications | 12/31/1999 | NGDC Data and System Administrators | |

**Core Business Process (CBP):Data Center Services(NGDC)**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| | | | | | | systems operate properly. | | | |

**Core Business Process (CBP):Telecommunications and Facilities (NCDC)**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.6.1.4 | Voice Telecommunications Outage - NCDC would be limited to communicate with its customers. | 01/01/2000 | .1 | 10 | 1.0 | a) Request vendor verification of Year 2000 compliance. | 07/31/1998 | NCDC (a-d) | a) In the event that the system router that distributes calls evenly among multiple customer services personnel is not operating properly on Jan. 1, 2000, contact vendor to repair and retest. |
| | | | | | | b)Telephone System found non-compliant | 08/31/1998 | | b) As an alternate until system is repaired, have vendor establish direct calling on multiple lines to customer servicing. (This plan implemented during prior failures of system). |
| | | | | | | c) Order vendor verified compliant system. | 02/28/1999 | | c) In the event of a building infrastructure systems failure, manual overrides will be applied until system correction can be made. |
| | | | | | | d) Install compliant system. | 03/31/1999 | | |

**Core Business Process (CBP):Telecommunications and Facilities (NCDC)**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.6.1.5 | Facility infrastructure is inoperable due to systems not being Year 2000 compliant - Utilize automated systems for such things as security environmental control, and elevators, etc. Date sensitive systems not made Year 2000 compliant risk being inoperable January 1, 2000. | 01/01/2000 | .1 | 10 | 1.0 | a)Participate with GSA to use vendor supplied information to check status of vendor products supporting automated infrastructure systems. | 09/30/1998 | GSA | 1) In the event of a building infrastructure system failure, manual overrides will be applied until system corrections can be made. |

**Core Business Process (CBP):Telecommunications and Facilities (NODC)**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.6.1.6 | Voice Telecommunications Outage -NODC would not be able to communicate with its customers. | 01/01/2000 | .1 | 10 | 1.0 | a) Request vendor verification of Year 2000 compliance. System non-compliant. | 09/23/1998 | NODC (a-d) | a) In the event that the system router that distributes calls evenly among multiple customer services personnel is not operating properly on Jan 1, 2000, contact vendor to repair and retest. |
| | | | | | | b) Order vendor verified compliant system. | 12/15/1998 | | |
| | | | | | | c) Install compliant system. | 01/15/1999 | | |
| | | | | | | d) Verify Voice Telecommunications system operating properly. | 01/30/1999 | | |
| 2.6.1.7 | Facility infrastructure is inoperable due to systems not being Year 2000 compliant -Utilize automated systems for such things as security, environmental control, and elevators, etc. Date sensitive systems not made Year 2000 compliant risk being inoperable January 1, 2000. | 01/01/2000 | .1 | 10 | 1.0 | a) Participate with GSA to use vendor supplied information to check status of vendor products supporting automated infrastructure systems. | 09/30/1998 | GSA | 1) In the event of a building infrastructure system failure, manual overrides will be applied until system corrections can be made. |

**Core Business Process (CBP):Telecommunications and Facilities (NODC)**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| | | | | | | b) Assess computer room combination lock for Y2K compliance. Identify manual overrides or alternative locks as part of assessment and validation. | 12/31/1998 | NODC | 2) If necessary NODC will install new computer room combination lock. |

**Core Business Process (CBP):Telecommunications and Facilities (NGDC)**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.6.1.8 | Voice/Telecommunications/voice mail outage - NGDC would not be able to communicate with its customers or would be hindered. | 01/01/2000 | .1 | 10 | 1.0 | a) NGDC requested vendor certification of system Year 2000 Compliance | 01/30/1998 | NIST Telecom Office | 1)Use cellular phone where possible.<br>2) Vendor (Northern Telecom) has stated that the Meridian Option 71 system is Y2K compliant. Voice mail option of the system will be upgraded before July 31, 1999. |
| 2.6.1.9 | Facility infrastructure is inoperable due to systems not being Y2K compliant | 01/01/2000 | .1 | 10 | 1.0 | a) NGDC is moving to a new 21st Century state of the art facility in February 1999 at 325 Broadway, Boulder, CO | 01/31/1997 | GSA | 1)Contractor/sub-contractor's have verified that all infrastructure systems are or will be Y2K compliant. |
| | | | | | | | | | 2)Any problems will be reported to the GSA Building Manager. |

**Core Business Process (CBP): Search and Rescue Satellite Aided Tracking**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Risk Mitigation Strategy | Milestone Dates | Action Component | |
| 2.6.2.1 | NESDIS is unable to send alert messages to US and international search and rescue authorities regarding distress signals sent by emergency beacons. | 12/31/1999 | .1 | 10 | 1.0 | a) Notify and work with all data exchange partners | Ongoing | OSDPD/ DSD (a-k) | 1) In the event that the Sarsat systems are unable to function the emergency response team will analyze the problem, make repair, and retest immediately. code. |
| | | | | | | b) Continue outreach and awareness efforts with customers and partners. | Ongoing | | 2) If some component of the Sarsat system does not appear to function normally following the year 1999 - 2000 transition, the February 28 - 29, year 2000 transition, or the day 365 - day 366, year 2000 transition, then the duty officer will assess the severity of the problem and call the emergency on-call individual responsible for the maintenance of that component. That individual will determine nature of and severity of the problem. The lead will then assign the appropriate emergency response resources needed to remedy the problem . Response time for corrective action will depend on the severity of the problem. |
| | | | | | | c) Complete renovation of mission | 09/30/1998 | | 3)In the event that a failure |

**Core Business Process (CBP): Search and Rescue Satellite Aided Tracking**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Risk Mitigation Strategy | Milestone Dates | Action Component | |
| | | | | | | critical systems: US Mission Control Center and Local User Terminals. | | | prevents the US Mission Control Center from performing its basic function of Cospas-Sarsat Data processing distribution, formal backup procedures as published in Cospas-Sarsat Documentation will be implemented. These procedures provide for foreign MCCs to fulfill the Nodal (international) and National requirements of the USMCC. |
| | | | | | | d) Develop Business Continuity and Contingency Plan. | 02/151999 | | |
| | | | | | | e) Coordinate test with Cospas-Sarsat partners; determine point-of-contact with each organizations; meet formally and determine points of failure, establish test procedures and schedule “live” test where practical and permitted. | 03/01/1999 | | |
| | | | | | | f) Prepare simulated data input where necessary. | Ongoing | | 2)Vendor has stated that Merlin II system is Year 2000 compliant. DSD/Sarsat does not have voice mail |
| | | | | | | g) Complete testing with forward dates set on all system components. | 03/31/1999 | | |
| | | | | | | h) Implement System | 03/31/1999 | | a)Implement Asynchronous LUT communications |

**Core Business Process (CBP): Search and Rescue Satellite Aided Tracking**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Risk Mitigation Strategy | Milestone Dates | Action Component | |
| | | | | | | | | | b)Implement FTS Fax and MCI Fax and manual Fax |
| | | | | | | I) Assign emergency response teams in anticipation of system failure. | 06/30/1999 | | c)implement email and FTP |
| | | | | | | j) Continue reporting progress and highlighting problems and successes. | Ongoing | | |
| | | | | | | k) Procure Y2K compliant COTS items to replace the COTS items that will not be Y2K compliant . | 03/31/1999 | | |
| 2.6.2.2 | Voice Telecommunications/voice mail outage - would not be able to communicate with its customers or would be hindered. | 12/31/1999 | .2 | 10 | 2.0 | Request vendor verification of Year 2000 compliance | 11/01/1998 | System Div/Telecom& ADP Security Br. | 1)Use cellular phones where possible.<br><br>2) DSD is determining resources needed o manually fix building key card system if necessary. |

**Core Business Process (CBP): Search and Rescue Satellite Aided Tracking**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Risk Mitigation Strategy | Milestone Dates | Action Component | |
| 2.6.2.3 | Data communications are inoperable - communications between search and rescue sites not functional | 12/31/1999 | .3 | 10 | 3.0 | The Sarsat system currently uses FTS 2000 X.25 service which may be discontinued in June 99. Sarsat personnel are inquiring this possible discontinuation and the Y2K compatible replacements. | Completed | | Failures of the X.25 link to the FTS cloud will require implementation of multiple contingencies built into the existing Cospas-Sarsat contingency plan. |
| 2.6.2.4 | Facility infrastructure is inoperable due to systems not being Year 2000 compliant - security, environmental control, and elevators, etc. | 12/31/1999 | .1 | 10 | 1.0 | a)Participate with GSA to use vendor supplied information to check status of vendor products supporting automated infrastructure systems. | 01/31/1999 | | 1) In the event of a building infrastructure system failure, manual overrides will be applied until system corrections can be made. |
| | | | | | | b) Identify manual overrides or alternative systems for building key card system as part of assessment and validation. | | | |

**Core Business Process (CBP): Satellite Operations**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.6.3.1 | GOES ground system capability to control spacecraft and/or to receive and process telemetry is impaired. | 12/31/1999 | .1 | 10 | 1.0 | a) Complete the renovation of the GOES ground system components.<br><br>b) Complete testing and validation of GOES ground system components.<br><br>c) Implement any Y2K renovations made and validated but not already in place. Apply any necessary vendor supplied patches or updates. | 09/30/1998<br><br>01/31/1999<br><br>02/28/1999 | OSO<br><br>OSO<br><br>OSO | 1) If some component of the GOES ground system does not appear to function normally following the year 1999 - 2000 transition, the February 28 - 29, year 2000 transition, or the day 365 - day 366, year 2000 transition, then the shift supervisor on duty will apprise the hardware/software lead for the maintenance of that component who is on-call. The lead will determine with the shift supervisor the nature of and severity of the problem. The lead will then assign the appropriate resources to remedying the problem in relation to the severity. The solution will be applied following existing CM procedures. In addition, contingency procedures are in place - see (Satellite Processing) to use alternative satellite data. |

**Core Business Process (CBP): Satellite Operations**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.6.3.2 | Polar Acquisition Control System (PACS) ground system capability to control spacecraft and/or to receive and process telemetry is impaired. | 12/31/1999 | .1 | 10 | 1.0 | a) Complete the renovation of the GOES ground system components.<br><br>b) Complete testing and validation of GOES ground system components.<br><br>c) Implement any Y2K renovations made and validated but not already in place. Apply any necessary vendor supplied patches or updates. | 09/30/1998<br><br>01/31/1999<br><br>02/28/1999 | OSO<br><br>OSO<br><br>OSO | 1) If some component of the POES ground system does not appear to function normally following the year 1999 - 2000 transition, the February 28 - 29, year 2000 transition, or the day 365 - day 366, year 2000 transition, then the shift supervisor on duty will apprise the hardware/software lead for the maintenance of that component who is on-call. The lead will determine with the shift supervisor the nature of and severity of the problem. The lead will then assign the appropriate resources to remedying the problem in relation to the severity. The solution will be applied following existing CM procedures. In addition, continency procedures are in place see (Satellite Processing) to use alternative satellite data. |

**Core Business Process (CBP): Satellite Operations**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.6.3.3 | Integrated Polar Acquisition Control (IPACS) ground system capability to control spacecraft and/or to receive and process telemetry is impaired. | 12/31/1999 | .1 | 10 | 1.0 | a) The contractor who built the ground system had a contractual obligation to deliver a Y2K compliant system.<br><br>b) The system was tested at the remote site, ESOC, for compliance. | Completed<br><br>Completed | OSD<br><br>OSD | 1) If some component of the IPACS ground system does not appear to function normally following the year 1999 - 2000 transition, the February 28 - 29, year 2000 transition, or the day 365 - day 366, year 2000 transition, then the shift supervisor on duty will apprise the hardware/software lead for the maintenance of that component who is on-call. The lead will determine with the shift supervisor the nature of and severity of the problem. The lead will then assign the appropriate resources to remedying the problem in relation to the severity. The solution will be applied following existing CM procedures. |

**Core Business Process (CBP): Satellite Operations**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.6.3.4 | GOES spacecraft | 12/31/1999 Based on ground system only. Spacecraft has no year or month dependant components. | .1 | 10 | 1.0 | a) Have spacecraft engineers evaluate spacecraft for possible time-dependant problems. | Completed. | OSO | 1) Spacecraft are monitored 24x7 for all problems. If any problem may cause a data outage, existing plans and procedures will be used. OSO spacecraft engineers are on 24 hour call to respond to spacecraft anomolies. In order to compensate for the loss of data from an effected spacecraft in the short term, 8-72 hours, the imagery schedule of another spacecraft may be changed. Engineers may move another spacecraft location to a central location to compensate for the loss of spacecraft data for periods of greater than 72 hours. |

**Core Business Process (CBP): Satellite Operations**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.6.3.5 | POES spacecraft | 12/31/1999 Based on ground system only. | .1 | 10 | 1.0 | a) Have spacecraft engineers evaluate spacecraft for possible time-dependant problems. | Completed. | OSO | 1) Spacecraft are monitored 24x7 for all problems. If any problem may cause a data outage, existing plans and procedures will be used. OSO spacecraft engineers are on 24 hour call to respond to spacecraft anomolies The POES spacecraft will continue to operate autonomously for several days while problems are evaluated and resolved. |
| 2.6.3.6 | DAPS Data Collection System (DCS) | 12/31/1999 | .1 | 5 | .5 | a) Complete the renovation of the GOES ground system components.<br><br>b) Complete testing and validation of GOES ground system components.<br><br>c) Implement any Y2K renovations made and validated but not already in place. Apply any vendor supplied patches or updates. | 09/30/1998<br><br>01/31/1999<br><br>02/28/1999 | OSO<br><br>OSO<br><br>OSO | a) The system will be monitored during the year 1999 - year 2000 and the year 2000 leap year. Any previously undiscovered problems will be resolved by a programmer at the WCDA where the system resides. Any software changes will be retested. |

**Core Business Process (CBP): Satellite Operations**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.6.3.7 | Telecomm | 12/31/1999 | .1 | 10 | 1.0 | Telecomm services were certified by the vendor. | Complete. | OSO | a) In the event that normal communications links with remote sites are not available, backup communications paths are in place.<br>In the event of further loss of communications remote sites can take over most of the functions of the SOCC. |
| 2.6.3.8 | Facilities | 12/31/1999 | .1 | 10 | 1.0 | a) Contact GSA concerning compliance issues of SOCC.<br><br>b) FCDAS and WCDAS contact contractors concerning compliance issues of facilities infrastructure. | 11/30/1998<br><br>11/30/1998 | GSA<br><br>OSO | a) Electrical backup generators provide electrical power if commercial power unavailable.<br><br>b) Remote sites can serve as backups to one another for brief periods.<br><br>c) Security access can be controlled manually if necessary. |
| 2.6.3.9 | Voice Telecommunication/voice mail outage would not be able to communicate with its customers or would be hindered | 12/31/999 | .2 | 10 | 2.0 | a) Request vendor certification of Y2K compliance | 11/30/1998 | Systems Division/Telecomm & ADP Security Branch | a) Use cellular phones where possible.<br><br>b) Vendor has certified that the Legend and Intuity voice-mail systems are compliant and was tested. |

**Core Business Process (CBP): Satellite Processing**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.6.4.1 | The Office of Satellite Data Processing and Distribution is unable to disseminate Polar data or products to customers | 12/31/1999 | .1 | 10 | 1.0 | a) Identify all data exchange partners and establish Memoranda of Agreement as necessary. | Completed | OSDPD/ICD (a-l) | 1) If some component of the Polar system does not appear to function normally following the year 1999 - 2000 transition, the February 28 - 29, year 2000 transition, or the day 365 - day 366, year 2000 transition, then the Product Production Leader on duty will notify the hardware/software lead for the maintenance of that component who is emergency on-call. The lead will determine with the Product Production Leader the nature of and severity of the problem. The lead will then assign the appropriate emergency response resources to remedy the problem. The solution will be applied using Standard Operating Procedures (SOP's) and existing Configuration Management (CM) practices. |
| | | | | | | b) Continue outreach and awareness efforts with customers and partners. | Ongoing | | 2)Coordinate with NESDIS OSO on trouble shooting the problem. |

**Core Business Process (CBP): Satellite Processing**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| | | | | | | c) Complete the renovation of all of the mission critical systems within Satellite Processing. | Completed | | 3) Notify users. |
| | | | | | | d) Develop Test Plan | Completed | | 4)Implement contingency plan for receipt of DoD satellite data and begin processing. |
| | | | | | | e) Establish Quality Assurance Team | Completed | | |
| | | | | | | f) Coordinate test with data exchange partners; determine point-of-contact with external organization; meet formally and determine points of failure, establish test procedures and schedule simulated tests | Completed | | |
| | | | | | | g) Develop Business Continuity and Contingency Plan. | 11/15/1998 | | |
| | | | | | | h) Create simulated test data sets | 12/31/1998 | | |
| | | | | | | i) Complete testing and validation of polar data or products | 01/31/1999 | | |
| | | | | | | j) Complete implementation | 03/31/1999 | | |
| | | | | | | k) Assign emergency response teams | 06/30/1999 | | |

**Core Business Process (CBP): Satellite Processing**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| | | | | | | l) Continue reporting progress and highlighting problems and successes. | Ongoing | | |
| 2.6.4.2 | The Office of Satellite Data Processing is unable to receive & disseminate Geostationary Satellite Data to customers | 12/31/1999 | .2 | 10 | 2.0 | a) Develop and implement a Replacement GOES Ingest NOAA-Port Interface (GINI) Ingest System | 03/31/1999 | GINI ReHost Team | 1) In the event of contingency being called to action, SSD will manage and prioritize problem solution according to 4 levels: |
| | | | | | | b) Complete test and validation of the new GINI Replacement System with incoming Satellite test data streams. | 03/31/1999 | | Level 1) Highest priority. Systems and functions at this level are essential to the continuation of SSD's critical business functions. Resources are immediately deployed to resolve issues and problems at this level. Resources from lower levels may also be deployed to provide additional assistance in expediting resolution. |

**Core Business Process (CBP): Satellite Processing**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| | | | | | | | | | Level 2) Systems and functions at this level are essential to the continued function of SSD's mission to provide support of life and property saving functions. Resources are made available after actions and personnel have been fully deployed to resolve level 1 issues |

**Core Business Process (CBP): Satellite Processing**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| | | | | | | | | | Level 3) Systems and functions at this level are important to the continuation of data products. Resources are made available after actions and personnel have been fully deployed to resolve Level 1 and Level 2 issues.<br><br>Level 4) Systems and functions at this level are organizational support systems and products. Resources are deployed after actions and personnel have been fully deployed to resolve Level 1, 2, and 3 issues.<br><br>Within each of the Triage Levels the systems will be ordered according to mission importance. Available resources will be deployed for resolution of issues and problems beginning with those systems and functions having the highest rating. |

**Core Business Process (CBP): Satellite Processing**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.6.4.3 | The Office of Satellite Data Processing and Distribution is unable to generate & distribute Geostationary Products. | 12/31/1999 | .2 | 8 | 1.6 | a) Complete Renovation | Completed | Y2K Technical Team | To mitigate risk resulting from controllable contingency condition, the SSD Y2K effort is structured to include the following. |
| | | | | | | b) Testing and Validation | 01/31/1999 | Y2K Test Team | Monthly management status meetings(include all branch managers, and function areas). |
| | | | | | | c) Y2K Day Test | 02/28/1999 | Y2K Test Team | Y2K Project Manager reports directly to the Division Director for matters concerning Y2K (an emergency meeting can be called at any time and Ben Watkins is notified at the first sign of a problem). |
| | | | | | | d) Implementation | 03/31/1999 | Y2K Technical Team | Schedules are updated and published in the Y2K Lotus Notes database, weekly. The Y2K conversion effort is continually monitored by the Y2K Core Team for conditions that would place us in a contingency condition. |

**Core Business Process (CBP): Satellite Processing**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| | | | | | | e) System Freeze | 11/15/1999 | Y2K Technical Team | Weekly status reports from programmers are submitted to management, outlining the most current status of the Y2K effort. |

**Core Business Process (CBP): Satellite Processing**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| | | | | | | f) Year 2000 Turnover | 12/31/1999 | Y2K Technical Team | Programmers meet weekly to discuss renovation issues, problems and schedules. 1) If some component of the GOES system does not appear to function normally following the year 1999-2000 transition, the February 28-29, year 2000 transition, or the day 365- day 366, year 2000 transition, then the Product Production Leader on duty will notify the hardware/software lead for the maintenance of that component who is on emergency on-call. The lead will determine with the Product Production Leader the nature of and severity of the problem. The lead will then assign the appropriate emergency response resources to remedy the problem.<br>2) Coordinate with NESDIS OSO on trouble shooting the problem.<br>3) Notify users4)Implement contingency plan for receipt of DoD satellite data and begin processing. |

**Core Business Process (CBP): Satellite Processing**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.6.4.4 | Voice Telecommunications Outage would not be able to communicate with its customers. | 12/31/1999 | .2 | 10 | 2.0 | Request vendor verification of Year 2000 compliance | 11/01/1998 | System Div /Telecom & ADP Security Br. | 1)Vendor has stated that Merlin II System is Year 2000 compliant. Satellite Processing does not have voice mail. |
| 2.6.4.5 | Data communications are inoperable - communications between the GOES and POES processing centers and the customers are inoperable. | 12/31/1999 | .1 | 10 | 1.0 | The distribution of GOES and POES data and products takes place of an intranet or via leased lines. The intranet lines are Y2K compliant and the equipment at each end is either already compliant or will be replaced with compliant equipment. The majority of OSDPDs outside customers are fed via Bell Atlantic lines which have been certified by the vendor as compliant. | 01/31/1999 | OSDPD | Failures of the intranet or of the leased lines will require implementation of multiple contingencies built into the OSDPD Standard Operating Procedures(SOP).<br>a) use backup comms lines<br>b) use direct broadcast via the satellite<br>c) point customers to NOAAs web sites for products and services.<br>d) implement the DoD/NOAA satellite contingency plan for the distribution of DoD satellite data to NOAA customers. |

**Core Business Process (CBP): Satellite Processing**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.6.4.6 | Facility infrastructure is inoperable due to systems not being Year 2000 compliant - Utilize automated systems for such things as security, environmental control, and elevators, etc. Date sensitive systems not made Year 2000 compliant risk being inoperable January 1, 2000. | 12/31/1999 | .1 | 5 | .5 | a) Participate with GSA to use vendor supplied information to check status of vendor products supporting automated infrastructure systems.<br><br>b) Identify manual overrides or alternative systems for building key card system as part of assessment and validation. | 09/30/1998<br><br>Completed 07/30/1998 | GSA<br><br>OSDPD/IPD | 1) In the event of a building infrastructure system failure, manual overrides will be applied until system corrections can be made.<br><br>2) Satellite Processing has identified resources to manually fix building key card system if necessary. |

**Core Business Process(CBP): Satellite Research**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.6.5.1 | NESDIS/ORA is unable to perform analyses or to provide satellite calibration information and derived scientific data to its users. | 01/01/2000 | .1 | 8 | .8 | a) Evaluate research programs and data exchange patterns for ORA scientists; establish emergency working plans as necessary. | Completed | NESDIS/ | 1) In the event that the ORA systems are unable to function the emergency response team will analyze the problem, make repair, and retest immediately. code. |
| | | | | | | b) Complete renovation of mission critical systems. | Completed | ORA System Emergency Response Team | 2) Delivery of analytical results to ORA's users will be completed using a legacy/manual methodology until corrections are made. |
| | | | | | | c) Develop Test Plan. | 12/31/1998 | | |
| | | | | | | d) Complete testing with forward dates set on all system components. | 01/31/1999 | | |
| | | | | | | e) Implement System | 03/31/1999 | | |
| | | | | | | f) Sensitize users in ORA to the Y2K problem and proper usage of dates in common usage and programming. | Ongoing | | |
| 2.6.5.2 | A) Voice Telecommunications outage - ORA unable to communicate with its users and NOAA management. | 01/01/2000 | .2 | 10 | 2.0 | a) Request vendor verification of Year 2000 compliance. | Completed | AT&T | 1)Use cellular phones where possible. Work with NOAA main line offices to assure continuity of phone systems. |

**Core Business Process(CBP): Satellite Research**

| MCS or CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| | | | | | | b) apply patch, or introduce upgrade to ensure compliance. | 06/30/1999 | Intuity Systems | 2) Work with Intuity Systems to assure patch is available; if no patch is offered, evaluate costs to proceed to a different voicemail system. Operate in the interim without. |
| | B) Intuity voicemail system is not working in year 2000. | 01/01/2000 | .5 | 2 | 1.0 | a) request vendor verification that Intuity system is Y2K compliant. | Completed | | |
| | | | | | | b) apply patch or introduce upgrade for compliance. | 06/30/1999 | | |
| 2.6.5.3 | Facility infrastructure inoperable due to systems not being Year 2000 compliant - The NOAA Science Center utilizes many automated systems for such things as security, environmental control, and elevators, etc. Date-sensitive systems risk being inoperable 01/01/2000. | 01/01/2000 | .1 | 8 | .8 | a) Work with NOAA Science Center Building Committee to assure that all surveys, assessments and planning documentation is completed; assist in developing contingency plans for the building; identify manual overrides or alternative systems for the building infrastructure systems as part of assessment and certification; and testing infrastructure systems to resolve any problems prior to opening for business 01/03/2000. | Ongoing | NSC Building Committee | 1) In the event of a building infrastructure system failure, manual overrides will be applied until system corrections can be made<br><br>.2) ORA will divert resources as needed to ensure corrections are made as soon as possible. |

**Core Business Process (CBP):NMFS Agency Management**

| CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.7.1.1 Agency Management | Managing Financial Resources Financial Reporting Systems (FRS) | 01/01/2000 | .1 | 10 | 1.0 | a. Develop Test Plan | 01/29/1999 | System Manager, Y2K Business Resumption Team (BRT) (a-e) | 1) In the event that the NMFS financial system -FRS- fails, the Y2K Business Resumption Team will analyze the problem and coordinate testing and fixing of the problem with the appropriate technical program administrators. |
| | NMFS is unable to use its information system to manage planning, budget formulation, budget execution, and financial reporting. | | | | | b. Date testing on Y2K test bed | 03/31/1999 | | 2) Data entry will be accomplished through standard Government paper forms which will be entered electronically after system corrections are made. |
| | | | | | | c. Continue outreach and awareness efforts with customers and partners | Ongoing | | 3) Financial reporting will be suspended until system corrections are made, or reports will be generated from the NOAA FIMA system. |
| | | | | | | d. Develop Contingency Plan | 02/1511999 | | |
| | | | | | | e. Assign priorities to Business Resumption Team | 07/01/1999 | | |

National Oceanic and Atmospheric Administration
Business Continuity and Contingency Plan
# NATIONAL MARINE FISHERIES SERVICE

**Core Business Process (CBP): Living Marine Resources Research and Regulation**

| CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.7.2.1 | Managing Critical Permits: Dealer Permits System<br><br>Permit Program Information Management System | 01/01/2000 | .1 | 7 | .7 | a. Develop Test Plan | 01/29/1999 | System Manager, Y2K Business Resumption Team (BRT) (a-e) | 1) In the event that these systems fail, the Y2K Business Resumption Team will analyze the failure and coordinate testing and fixing the problem with the systems developers. |
| | NMFS is unable to process and monitor critical permits. | | | | | b. Implement Test Plan | 03/31/1999 | | 2) Permit processing and monitoring will be accomplished through standard Government paper forms which will be entered electronically after system corrections are made. |
| | | | | | | c. Continue outreach and awareness efforts with customers and partners | Ongoing | | 3) Reporting on the status of permits will be suspended until system corrections are made. |
| | | | | | | d. Develop Contingency Plan | 03/31/1999 | | |
| | | | | | | e. Assign priorities to Business Resumption Team | 07/01/1999 | | |

**Core Business Process (CBP): Living Marine Resources Research and Regulation**

| CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.7.2.2 Living Marine Resources Research and Regulation | NMFS is unable to access any of the remaining 67 mission critical systems | 01/01/2000 | .1 | 7 | .7 | a. Develop Test Plan | 01/29/1999 | System Manager, Y2K Business Resumption Team (BRT) (a-e) | 1) In the event that these NMFS systems fail, the Y2K Business Resumption Team will analyze the failure, determine if other NMFS servers can re-host the server and documents and fix the problem. Normal Internet web hosting will be suspended until the server can be fixed. |
| | | | | | | b. Implement Test Plan | 03/31/1999 | | 2) Data entry will be accomplished through standard Government paper forms which will be entered electronically after system corrections are made. |
| | | | | | | c. Continue outreach and awareness efforts with customers and partners | Ongoing | | 3) Reports and other output from these systems will suspended until system corrections are made. |
| | | | | | | d. Develop Contingency Plan | 03/31/1999 | | |
| | | | | | | e. Assign priorities to Business Resumption Team | 07/01/1999 | | |

**Core Business Process (CBP): Telecommunications and Facilities**

| CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.7.3.1 | Voice Telecommunications Outage - NMFS would not be able to communicate with its customers | 01/01/2000 | .2 | 10 | 2.0 | Request vendor verification of Y2K compliance, apply patch, or introduce upgrade to ensure compliance | 12/30/1999 | System Div./ Telecom. & ADP Security Branch | |

**Core Business Process (CBP): Telecommunications and Facilities**

| CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| 2.7.3.2 | Facility infrastructure is inoperable due to systems not being Y2K compliant. Many of NMFS buildings utilize automated systems for such things as security, environmental control, elevators, etc. Date sensitive systems not made Y2K compliant risk being inoperable January 1, 2000. | 01/01/2000 | .1 | 10 | 1.0 | A. Complete the NMFS facility surveys. | 09/30/1998 | AGFS/FMD | 1) In the event of a building infrastructure system failure, manual overrides will be applied until system corrections can be made. |
| | | | | | | B. Participate with GSA to use vendor supplied information to check status of vendor products supporting automated infrastructure systems. | 09/30/1998 | | 2) NMFS will divert resources to ensure corrections are made as soon as possible. |
| | | | | | | C. Develop contingency plans for Washington, D.C. buildings and Field Locations. | Ongoing | | |

**Core Business Process (CBP): Telecommunications and Facilities**

| CBP# | Risk/Threat | Time Horizon to Failure | Business Priority | | | Risk Mitigation Strategy | | | Contingency Plan and Triggers |
|---|---|---|---|---|---|---|---|---|---|
| | | | Risk Assess. | Impact | Score | Mitigation Strategy | Milestone Dates | Action Component | |
| | | | | | | D. Identify manual overrides or alternative systems for building infrastructure systems as part of assessment and certification. | 12/30/1998 | | |
| | | | | | | E. Identify any infrastructure Y2Kproblems on the first working day of Year 2000. | 01/03/2000 | | |